

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-46856

(P2004-46856A)

(43) 公開日 平成16年2月12日(2004.2.12)

(51) Int. Cl. <sup>7</sup>

G06F 12/14  
H04L 9/08  
H04L 9/32

F 1

G06F 12/14 310K  
H04L 9/00 675B  
H04L 9/00 675D  
H04L 9/00 675Z  
H04L 9/00 601E

テーマコード(参考)

5B017  
5J104

審査請求 未請求 請求項の数 28 O L (全 41 頁)

(21) 出願番号 特願2003-183596 (P2003-183596)  
(22) 出願日 平成15年6月26日(2003.6.26)  
(31) 優先権主張番号 10/185,527  
(32) 優先日 平成14年6月28日(2002.6.28)  
(33) 優先権主張国 米国(US)

(71) 出願人 391055933  
マイクロソフト コーポレーション  
MICROSOFT CORPORATI  
ON  
アメリカ合衆国 ワシントン州 9805  
2-6399 レッドモンド ワン マイ  
クロソフト ウェイ (番地なし)  
(74) 代理人 100077481  
弁理士 谷 義一  
(74) 代理人 100088915  
弁理士 阿部 和夫  
(72) 発明者 スティーブン ボーン  
アメリカ合衆国 98122 ワシントン  
州 シアトル イースト パイク ストリ  
ート 303 ナンバー602  
最終頁に続く

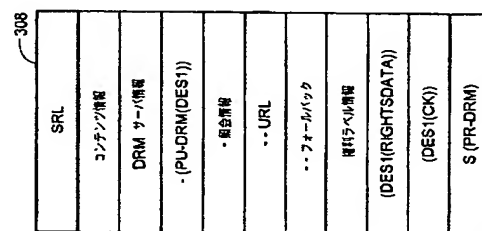
(54) 【発明の名称】 デジタルコンテンツに対応するデジタルライセンスを取得する方法

## (57) 【要約】

【課題】コンテンツは、コンテンツ鍵(CK)に従って暗号化され(CK(content))、(CK)は、ライセンスサーバの公開鍵(PU-DRM)に従って保護され、コンテンツに関連する権利データは、(PU-DRM)に従って保護される。

【解決手段】これら保護された項目は、ライセンスサーバによる署名を受けるために、権利ラベルとしてライセンスサーバに提出される。ライセンスサーバは、権利ラベルが有効か否かを検査し、有効であれば、保護された権利データに基づいてデジタル署名し、その結果として署名付き権利ラベル(SRL)を得て、権利ラベルを戻す。SRLは、(CK(content))と連結され、両方をユーザに配信する。コンテンツをレンダリングするために、ユーザは、SRLをライセンスサーバに提出してライセンスを要求する。

【選択図】 図5



## 【特許請求の範囲】

## 【請求項1】

デジタルコンテンツを公表し、ライセンスサーバが前記コンテンツに対応するライセンスを、前記コンテンツをレンダリングすることを望む1または複数のユーザに発行することを可能にする方法であって、

コンテンツ鍵 (CK) に従って前記コンテンツを暗号化し、その結果として (CK (content)) を得ること、

前記ライセンスサーバの公開鍵 (PU-DRM) に従って前記コンテンツ鍵 (CK) を保護すること、

前記コンテンツに関連する権利データを生成すること、

(PU-DRM) に従って前記権利データを保護すること、

前記保護された権利データと前記保護されたコンテンツ鍵 (CK) とを権利ラベルとして、前記ライセンスサーバによる署名を受けるために、前記ライセンスサーバに提出し、前記ライセンスサーバは、前記権利ラベルが有効か否かを検査し、有効ならば、(PU-DRM) に対応する秘密鍵 (PR-DRM) に基づいた、おおよしくとも前記保護された権利データの一部に基づいたデジタル署名を生成し、その結果として署名付き権利ラベル (SRL) を得て、該 SRL を戻すこと、

前記戻された SRL を受け取り、前記受け取った SRL を (CK (content)) と連結してコンテンツパッケージを形成すること、おおよしく

前記コンテンツパッケージを前記1または複数のユーザに配信することにより、前記コンテンツをレンダリングすることを望むユーザは、前記コンテンツパッケージから前記 SRL を取り出し、取り出された SRL を前記コンテンツに対応する前記ライセンスの要求の一部として前記ライセンスサーバに提出し、前記ライセンスサーバは、(PU-DRM) に基づいて、おおよしくとも前記保護された権利データの一部に基づいて前記 SRL の署名を検査し、前記 SRL 内の前記保護された権利データにアクセスし、該権利データをレビューして、前記ユーザがライセンスを受ける権利があるか否かを判断し、そうであれば、前記ユーザにライセンスを発行し、前記ライセンスは、ユーザにアクセス可能に保護された形で (CK) を含むこと

を備えたことを特徴とする方法。

## 【請求項2】

前記ライセンスサーバの公開鍵 (PU-DRM) に従って前記コンテンツ鍵 (CK) を保護することは、

対称鍵 (DES1) を生成すること、

(DES1) に従って (CK) を暗号化し、その結果として (DES1 (CK)) を得ること、おおよしく

(PU-DRM) に従って (DES1) を暗号化し、その結果として (PU-DRM (DES1)) を得ることにより、前記ライセンスサーバは、(PR-DRM) を使用して (CK) にアクセスすることができること

を備えたことを特徴とする請求項1に記載の方法。

## 【請求項3】

(DES1) に従って (CK) を暗号化し、その結果として (DES1 (CK)) を得た後に、(CK) を破棄することにより、(CK) を、(DES1 (CK)) を解読することによってのみ取得できることをさらに備えたことを特徴とする請求項2に記載の方法。

## 【請求項4】

(PU-DRM) に従って前記権利データを保護することは、

対称鍵 (DES1) を生成すること、

(DES1) に従って前記権利データを暗号化し、その結果として (DES1 (right data)) を得ること、おおよしく

(PU-DRM) に従って (DES1) を暗号化し、その結果として (PU-DRM (DES1)) を得ることにより、前記ライセンスサーバは、(PR-DRM) を使用して (

10

20

30

40

50

ＣＫ）にアクセスすることができると  
を備えたことを特徴とする請求項１に記載の方法。

【請求項５】

対称コンテンツ鍵（ＣＫ）に従って前記コンテンツを暗号化し、その結果として（ＣＫ（*content*））を得ることを備えたことを特徴とする請求項１に記載の方法。

【請求項６】

前記コンテンツをレンダリングする権利を有する各エンティティと、各エンティティについて、前記エンティティが前記コンテンツをレンダリングすることに対して所持する各権利を含む権利データを生成することを備え、各エンティティは、ユーザおよびユーザクラスの１つを備えたことを特徴とする請求項１に記載の方法。

10

【請求項７】

前記権利のうちの少なくとも一部の各々について、前記コンテンツをレンダリングすることに対して、前記権利を実施するための前提条件を有する前記エンティティを含む権利データを生成することを備えたことを特徴とする請求項６に記載の方法。

【請求項８】

前記保護された権利データ、前記保護されたコンテンツ鍵（ＣＫ）、および権利ラベルとしてそのＩＤを含んでいる前記コンテンツに関する情報を、前記ライセンスサーバによる署名を受けるために、前記ライセンスサーバに提出することを備えたことを特徴とする請求項１に記載の方法。

【請求項９】

前記ライセンスサーバは、前記ライセンスサーバの所在を見つけるためのアドレス情報を含む、前記ライセンスサーバ上の前記権利ラベル情報を追加し、前記サーバに関する情報を含むＳＲＬを戻し、前記方法は、前記サーバに関する情報を含む、前記戻されたＳＲＬを受け取ることを備えたことを特徴とする請求項１に記載の方法。

20

【請求項１０】

ライセンスサーバからユーザにデジタルライセンスを提供する方法であって、前記ライセンスは、ユーザが対応する公表されたデジタルコンテンツをレンダリングすることを可能にし、前記コンテンツは、コンテンツ鍵（ＣＫ）に従って暗号化され、その結果として（ＣＫ（*content*））を得て、該（ＣＫ（*content*））は、前記ライセンスサーバの公開鍵（*PU-DRM*）に従って保護された（ＣＫ）と、（*PU-DRM*）に従って保護された権利データと、（*PU-DRM*）に対応する秘密鍵（*PR-DRM*）に基づいた、および少なくとも前記保護された権利データの一部に基づいたデジタル署名とを含む署名付き権利ラベル（*SR-L*）により付随して生じ、該方法は、前記ＳＲＬとユーザ鍵とを、前記ユーザから前記ライセンスの要求の一部として受け取ること、

30

前記ＳＲＬ内の署名にアクセスすること、

（*PU-DRM*）に基づいた、および少なくとも前記保護された権利データの一部に基づいた前記署名を検査すること、

前記ＳＲＬ内の前記保護された権利データにアクセスすること、

前記アクセスされた権利データをレビューして、ユーザが前記ライセンスを受ける権利があるか否かを判断すること、および

40

もしそうであれば、

前記ＳＲＬ内の前記保護された（ＣＫ）にアクセスし、

前記アクセスされた（ＣＫ）を前記受け取ったユーザ鍵に従って保護し、

前記ライセンスを前記ユーザに発行し、前記ライセンスは、前記ユーザ鍵に従って保護された（ＣＫ）を含み、これにより、前記ユーザは、前記ライセンスから（ＣＫ）にアクセスし、（ＣＫ）を（ＣＫ（*content*））に適用し、その結果としてコンテンツが得られること

を備えたことを特徴とする方法。

【請求項１１】

50

ライセンスサーバの公開鍵 (P U - D R M) に従って保護された (C K) は、対称鍵 (D E S 1) に従って暗号化され、その結果として (D E S 1 (C K)) を得る (C K) と、(P U - D R M) に従って暗号化され、その結果として (P U - D R M (D E S 1)) を得る (D E S 1) とを備え、該方法は、

(P R - D R M) を (P U - D R M (D E S 1)) に適用し、その結果として (D E S 1) を得ることと、

(D E S 1) を (D E S 1 (C K)) に適用し、その結果として (C K) を得ることにより、

前記 S R L 内の前記保護された (C K) にアクセスすること

を備えたことを特徴とする請求項 10 に記載の方法。

10

#### 【請求項 12】

(P U - D R M) に従って保護された前記権利データは、対称鍵 (D E S 1) に従って暗号化され、その結果として (D E S 1 (r i g h t s d a t a)) を得る権利データと、(P U - D R M) に従って暗号化され、その結果として (P U - D R M (D E S 1)) を得る (D E S 1) とを備え、該方法は、

(P R - D R M) を (P U - D R M (D E S 1)) に適用し、その結果として (D E S 1) を得ることと、

(D E S 1) を (D E S 1 (r i g h t s d a t a)) に適用し、その結果として権利データを取得することにより、

前記 S R L 内の前記保護された権利データにアクセスすること

を備えたことを特徴とする請求項 10 に記載の方法。

20

#### 【請求項 13】

前記 S R L およびユーザの公開鍵 (P U - U S E R) を、前記ユーザからの前記ライセンスの要求の一部として受け取ることとを備え、前記ユーザが前記ライセンスを受ける権利がある場合には、前記アクセスされた (C K) を、前記受け取った (P U - U S E R) に従って暗号化し、その結果として (P U - U S E R (C K)) を得て、(P U - U S E R (C K)) を含む前記ライセンスを前記ユーザに発行し、これにより、前記ユーザは、(P U - U S E R) に対応する秘密鍵 (P R - U S E R) を (P U - U S E R (C K)) に適用し、その結果として (C K) を得ることにより、前記ライセンスから (C K) にアクセスすることができ、(C K) を (C K (c o n t e n t)) に適用し、その結果としてコンテンツを得ることを特徴とする請求項 10 に記載の方法。

30

#### 【請求項 14】

前記アクセスされた権利データは、前記コンテンツをレンダリングする権利を有する各エンティティと、各エンティティについて、前記エンティティが前記コンテンツをレンダリングすることに対して所持する各権利とを含み、前記方法は、前記アクセスされた権利データをレビューして、前記要求するユーザが前記コンテンツをレンダリングする権利を有するユーザであるか否かを判断することと、そうであれば、前記ライセンスを前記ユーザに発行することとを備え、前記ライセンスは、前記コンテンツをレンダリングすることに対して、前記権利データに基づいて前記ユーザが有する各権利を含むことを特徴とする請求項 10 に記載の方法。

40

#### 【請求項 15】

前記アクセスされた権利データは、前記権利のうちの少なくとも一部の各々について、前記コンテンツをレンダリングすることに対して、前記権利を実施するための前提条件を有する前記エンティティを含み、前記方法は、前記要求するユーザが前記コンテンツをレンダリングする権利を有するユーザであれば、前記ライセンスを前記ユーザに発行することとを備え、前記ライセンスは、前記コンテンツをレンダリングすることに対して、前記権利データに基づいて前記ユーザが有する各権利と、各々の権利について、前記権利データに基づいて権利を実施するための前提条件とを含むことを特徴とする請求項 14 に記載の方法。

#### 【請求項 16】

50

デジタルコンテンツと、該コンテンツに対応し、前記コンテンツをレンダリングするためにライセンスサーバによりユーザに発行されたデジタルライセンスとを組み合わせた方法であって、

前記コンテンツは、コンテンツ鍵 (CK) に従って暗号化され、その結果として (CK (content)) を得て、該 (CK (content)) は、対称鍵 (DES1) に従って暗号化され、その結果として (DES1 (CK)) を得る (CK) と、対称鍵 (DES1) に従って暗号化され、その結果として (DES1 (rightdata)) を得る権利データと、ライセンスサーバの公開鍵 (PU-DRM) に従って暗号化され、その結果として (PU-DRM (DES1)) を得る (DES1) と、(PU-DRM) に対応する秘密鍵 (PR-DRM) に基づいた、および少なくとも (DES1 (rightdata)) の一部に基づいたデジタル署名とを含む署名付き権利ラベル (SRL) により付随して生じ、

前記ライセンスは、ユーザ鍵に従って保護された (CK) を含むことにより、前記ユーザは、前記ライセンスから (CK) にアクセスすることができ、(CK) を (CK (content)) に適用し、その結果として前記コンテンツを得て、前記ライセンスは、前記ユーザ鍵に従って暗号化された (DES1) をさらに含み、

前記ユーザが前記 SRL 内の前記権利データを変更する方法は、

前記ユーザ鍵に従って暗号化された (DES1) を前記ライセンスから取り出すこと、

前記ユーザ鍵に従って暗号化された (DES1) を解読し、その結果として (DES1) を得ること、

(DES1 (rightdata)) を前記 SRL から取り出すこと、

(DES1) を (DES1 (rightdata)) に適用し、その結果として前記権利データを得ること、

前記権利データを望み通りに変更すること、

変更された権利データを (DES1) に従って暗号化し、その結果として (DES1 (alterredrightdata)) を得ること、

(DES1 (alterredrightdata)) と (DES1 (CK)) を再公表権利ラベルとして、ライセンスサーバによる署名を受けるために、前記ライセンスサーバに提出し、前記ライセンスサーバは、前記再公表権利ラベルが有効か否かを検査し、有効ならば、(PR-DRM) に基づいた、および少なくとも (DES1 (alterredrightdata)) の一部に基づいたデジタル署名を作成し、その結果として署名付き再公表権利ラベル (SRR) を得て、該 SRR を戻すこと、

前記戻された SRR を受け取り、前記受け取った SRR を (CK (content)) と連結してコンテンツパッケージを形成すること、および

前記コンテンツパッケージを前記 1 または複数のユーザに配信することにより、前記コンテンツをレンダリングすることを望むユーザは、前記コンテンツパッケージから前記 SRL を取り出し、取り出した SRL を前記コンテンツに対応する前記ライセンスの要求の一部として前記ライセンスサーバに提出し、前記ライセンスサーバは、(PU-DRM) に基づいて、および少なくとも (DES1 (alterredrightdata)) の一部に基づいて前記 SRR の署名を検査し、前記 SRR 内の (DES1 (alterredrightdata)) にアクセスし、該 (DES1 (alterredrightdata)) をレビューして、前記ユーザがライセンスを受ける権利があるか否かを判断し、そうであれば、前記ユーザにライセンスを発行し、前記ライセンスは、ユーザにアクセス可能な保護された形式 (CK) を含むこと

を備えたことを特徴とする方法。

【請求項 17】

前記戻された SRR を受け取り、(CK (content)) から前記 SRL を取り除き、前記受け取った SRR を (CK (content)) と連結してコンテンツパッケージを形成することを備えたことを特徴とする請求項 16 に記載の方法。

【請求項 18】

10

20

30

40

50

前記ライセンスは、前記ユーザの公開鍵（P U - U S E R）に従って暗号化され、その結果として（P U - U S E R（C K））を得る（C K）、および（P U - U S E R）に従って暗号化され、その結果として（P U - U S E R（D E S 1））を得る（D E S 1）を含み、前記方法は、

（P U - U S E R（D E S 1））を前記ライセンスから取り出すこと、および（P U - U S E R（D E S 1））を（P U - U S E R）に対応する前記ユーザの秘密鍵（P R - U S E R）に従って解読し、その結果として（D E S 1）を得ることを含むことを特徴とする請求項 16 に記載の方法。

【請求項 19】

デジタルコンテンツを自己公表し、ライセンスサーバが前記コンテンツに対応するライセンスを、前記コンテンツをレンダリングすることを望む 1 または複数のユーザに発行することを可能にする方法であって、

公開鍵（P U - C E R T）と、前記ユーザの公開鍵（P U - C E R T）に従って暗号化され、その結果として（P U - U S E R（P R - C E R T））を得る、対応する秘密鍵（P R - C E R T）とを含む許可証明書を前記ライセンスサーバから受け取り、前記許可証明書は、前記ライセンスサーバの秘密鍵（P R - D R M）によって署名されていること、前記コンテンツをコンテンツ鍵（C K）に従って暗号化し、その結果として（C K（c o n t e n t））を得ること、

前記コンテンツ鍵（C K）を（P R - D R M）に対応する前記ライセンスサーバの公開鍵（P U - D R M）に従って保護すること、

前記コンテンツに関連する権利データを生成すること、

権利データを（P U - D R M）に従って保護すること、

前記保護された権利データと前記保護されたコンテンツ鍵（C K）とを権利ラベルとして提出すること、

前記受け取られた許可証明書から（P R - C E R T）を取得すること、

前記提出された権利ラベルを、少なくとも前記保護された権利データに基づいて取得された（P R - C E R T）で署名し、その結果として署名付き権利ラベル（S R L）を得ること、

前記 S R L および前記許可証明書と（C K（c o n t e n t））とを連結してコンテンツパッケージを形成すること、および

前記コンテンツパッケージを前記 1 または複数のユーザに配信することにより、前記コンテンツをレンダリングすることを望むユーザは、前記コンテンツパッケージから前記 S R L および前記許可証明書を取り出し、取り出された S R L および許可証明書を前記コンテンツに対応する前記ライセンスの要求の一部として前記ライセンスサーバに提出し、前記ライセンスサーバは、（P U - D R M）に基づいて前記証明書の署名を検査し、前記証明書から（P U - C E R T）を取得し、取得された（P U - C E R T）に基づいた S R L の署名を検査し、前記 S R L 内の前記保護された権利データにアクセスし、該権利データをレビューして、前記ユーザがライセンスを受ける権利があるか否かを判断し、そうであれば、前記ユーザにライセンスを発行し、前記ライセンスは、ユーザにアクセス可能に保護された形で（C K）を含むこと

を備えたことを特徴とする方法。

【請求項 20】

前記受け取られた許可証明書から（P R - C E R T）を取得することは、前記証明書から（P U - U S E R（P R - C E R T））を取得し、（P U - U S E R）に対応するユーザの秘密鍵（P R - U S E R）を（P U - U S E R（P R - C E R T））し、その結果として（P R - C E R T）を得ることを備えたことを特徴とする請求項 19 に記載の方法。

【請求項 21】

前記コンテンツ鍵（C K）を前記ライセンスサーバの公開鍵（P U - D R M）に従って保護することは、

対称鍵（D E S 1）を生成すること、

10

20

30

40

50

(CK)を(DES1)に従って暗号化し、その結果として(DES1(CK))を得ること、および

(DES1)を(PU-DRM)に従って暗号化し、その結果として(PU-DRM(DES1))を得ることにより、前記ライセンスサーバは、(PR-DRM)を使用して(CK)にアクセスすることができること

を備えたことを特徴とする請求項19に記載の方法。

【請求項22】

(DES1)に従って(CK)を暗号化し、その結果として(DES1(CK))を得た後に、(CK)を破棄することにより、(CK)を、(DES1(CK))を解読することによってのみ取得できることをさらに備えた特徴とする請求項21に記載の方法。

10

【請求項23】

(PU-DRM)に従って前記権利データを保護することは、

対称鍵(DES1)を生成すること、

(DES1)に従って前記権利データを暗号化し、その結果として(DES1(ハッシュα))を得ること、および

(PU-DRM)に従って(DES1)を暗号化し、その結果として(PU-DRM(DES1))を得ることにより、前記ライセンスサーバは、(PR-DRM)を使用して(CK)にアクセスすることができること

を備えたことを特徴とする請求項19に記載の方法。

【請求項24】

対称コンテンツ鍵(CK)に従って前記コンテンツを暗号化し、その結果として(CK(コンテンツ))を得ることを備えたことを特徴とする請求項19に記載の方法。

20

【請求項25】

前記コンテンツをレンタルする権利を有する各エンティティと、各エンティティについて、前記エンティティが前記コンテンツをレンタルすることに対して所持する各権利とを含む権利データを生成することを備え、各エンティティは、ユーザおよびユーザクラスの1つを備えたことを特徴とする請求項19に記載の方法。

【請求項26】

前記権利のうちの少なくとも一部の各々について、前記コンテンツをレンタルすることに対して、前記権利を実施するための前提条件を有する前記エンティティを含む権利データを生成することを備えたことを特徴とする請求項25に記載の方法。

30

【請求項27】

前記保護された権利データ、前記保護されたコンテンツ鍵(CK)、および権利ラベルとしてそのIDを含んでいる前記コンテンツに関する情報を、前記ライセンスサーバによる署名を受けるために、前記ライセンスサーバに提出することを備えたことを特徴とする請求項19に記載の方法。

【請求項28】

前記ライセンスサーバは、前記ライセンスサーバの所在を見つけるためのアドレス情報を含む、前記ライセンスサーバ上の前記権利ラベル情報を追加することを備えたことを特徴とする請求項19に記載の方法。

40

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル権利管理(DRM: digital rights management)システムに関する。より詳細には、本発明は、デジタルコンテンツの一部に対する署名付き権利ラベル(SRL: signed rights label)をライセンスサーバから取得する際に実行されるステップ、およびコンテンツに対応するデジタルライセンスをライセンスサーバから取得する際に実行されるステップに関する。

【0002】

【従来の技術】

50

デジタル権利の管理と実施は、デジタルオーディオ、デジタルビデオ、デジタルテキスト、デジタルデータ、デジタルマルチメディアなどのデジタルコンテンツに関連して高く望まれている。ここで、このようなデジタルコンテンツは、1または複数のユーザに配信されている。デジタルコンテンツは、例えば、テキストドキュメントなど静的なものもある。ライブイベントのストリーム型オーディオ／ビデオなどストリーム化されているものもある。代表的な配信モードには、磁気（フロッピー（登録商標））ディスク、磁気テープ、光（コンパクト）ディスク（CD）などの有形デバイスと、電子掲示板、電子ネットワーク、インターネットなどの無形メディアとがある。デジタルコンテンツがユーザによって受信されると、ユーザは、パーソナルコンピュータ等のメディアプレーヤなどの、適当なレンダリングデバイスの助けを借りて、デジタルコンテンツをレンダリングし、または「プレイ」する。

10

#### 【0003】

あるシナリオでは、著者、出版者、放送者などの、コンテンツ所有者または権利所有者は、ライセンス料または他の何らかの対価と引き換えに、デジタルコンテンツを多数のユーザまたは受取人の各々に配信することを望んでいる。このようなシナリオでは、コンテンツは、歌曲、アルバム、映画などがあり、ライセンス料を生み出すことが配信の目的である。このようなコンテンツ所有者は、選択権が与えられていれば、ユーザが、このように配信されたデジタルコンテンツを扱うことに対して制限を設けたいと望むであろう。例えば、コンテンツ所有者は、少なくとも別のユーザからのライセンス料を受け取らないで、ユーザがコンテンツをコピーし、別のユーザに再配信するのを制限したい。

20

#### 【0004】

さらに、コンテンツ所有者は、ユーザに異なる種類の使用ライセンスを異なるライセンス料で購入する柔軟性を与えると同時に、ユーザを実際に購入されたどの種類のライセンスの条項で拘束するか柔軟性を与えることを望む場合がある。例えば、コンテンツ所有者は、配信されたデジタルコンテンツを、制限された回数だけ、ある時間だけ、ある装置の種類だけ、あるメディアプレーヤの種類だけ、あるユーザの種類だけプレイできるようにすることを望む場合がある。

#### 【0005】

別のシナリオでは、企業内の従業員などのコンテンツ開発者は、そのデジタルコンテンツを、企業内の1または複数の他の従業員または企業外の他の個人に配信することを望むが、他人にコンテンツをレンダリングさせないことを望む場合がある。ここでは、コンテンツの配信は、ライセンス料または他の何らかの対価と引き換えに広く配信するのとは異なり、企業におけるコンテンツを機密または制限された形で共有するのとは似ている。このシナリオでは、コンテンツは、ドキュメントプレゼンテーション、スプレッドシート、データベース、電子メールなどであり、オフィス施設内でやりとりされる。コンテンツ開発者は、コンテンツがオフィス施設内に留まっていて、例えば、競業者または敵対者などの無許可の個人によりレンダリングされないことが保障されることを望む場合がある。このとき、そのコンテンツ開発者は、配信されたデジタルコンテンツを受取人がどのように扱うかについて制限を設けることを望んでいる。例えば、コンテンツ所有者は、少なくともコンテンツをレンダリングすることを許されている個人の範囲外にコンテンツが公開される方法で、ユーザがそのコンテンツをコピーし、別のユーザに再配信するのを制限したいと望んでいる。

30

40

#### 【0006】

さらに、コンテンツ開発者は、異なるレベルでレンダリングする権利を、種々の受取人に与えたいと望む場合がある。例えば、コンテンツ開発者は、保護されたデジタルコンテンツを、あるクラスの個人に対しては表示可能・印刷不能にし、別のクラスの個人に対しては表示可能・印刷可能にすると望む場合がある。

#### 【0007】

しかし、どちらのシナリオの場合も、配信が行われた後は、そのコンテンツ所有者／開発者は、デジタルコンテンツに対して制御できたとしても、その制御は無に等しい。このこ

50



とが特に問題となっているのは、ほとんどのパーソナルコンピュータも、デジタルコンテンツをそのままデジタルコピーし、そのデジタルコピーを、書き込み可能な磁気または光ディスクにダウンロードし、またはそのデジタルコピーを、インターネットなどのネットワーク経由で別のデスティネーションへ送信するのに必要なソフトウェアとハードウェアとを備えているからである。

#### 【0008】

当然のことであるが、コンテンツが配信されるトランザクションの一部として、コンテンツ所有者／開発者は、デジタルコンテンツのユーザ／受取人に要求して、そのデジタルコンテンツを望ましくない方法で再配信しないとの約束をすることができる。しかし、このような約束は容易に行われ、容易に破られる。コンテンツ所有者／開発者は、いくつかの公知のセキュリティデバイスのいずれかを通して、このような再配信を禁止することを試みることができ、通常は、暗号化と暗号解読が伴う。しかし、優柔不断なユーザ（*mildly determined user*）が暗号化デジタルコンテンツを解読し、そのデジタルコンテンツを非暗号化形式でセーブした後、その再配信を防止できる見込みはほとんどない。

#### 【0009】

##### 【発明が解決しようとする課題】

任意形態のデジタルコンテンツの制御されたレンダリングまたはフレイを行うことを可能にするデジタル権利管理、実施アーキテクチャ及びその方法を提供することが要望され、その制御は、フレキシブルで、そのデジタルコンテンツのコンテンツ所有者／開発者によって定義可能である。より具体的には、特にオフィス、組織環境、またはドキュメントが特定の個人グループまたは特定の個人クラスの間で共有されるような、制御されたレンダリングを行うことを可能にし、容易にするアーキテクチャが要望されている。

#### 【0010】

##### 【課題を解決するための手段】

本発明は、デジタルコンテンツとサービスの使用ライセンスを、署名付き権利ラベル（*SL*）を介して、発行するシステムと方法を提供することによって、「従来の技術」の個所で上述した要求を解決している。

#### 【0011】

本発明によれば、デジタル権利管理（*DRM*）ライセンス発行コンポーネントは、別のソフトウェアアプリケーションまたはコンポーネントが、ライセンスによって規定された条項に従ってデジタルコンテンツまたはサービスを消費するのを可能にするライセンスを発行する。ライセンスを発行するために、ライセンス発行コンポーネントは、一組の条項を規定している権利ラベルを使用し、その条項から1つの特定ライセンスを発行することを可能にしている。ライセンス条項は、コンテンツまたはサービスを使用する権利、条件、および本人を規定している。ここで用いられている「権利」という用語は、消費側コンポーネントによって理解される特定の動作である（例えば、デジタルメディアプレーヤーでは「フレイ」、ドキュメント管理システムでは「編集」）。ここで用いられている「条件」という用語は、消費側コンポーネントがその消費を行うのを許可する前に満たされていない場合にはならない特定の基準である（例えば、「12月1日より遅くない」）。さらに、ライセンスには、ライセンスの対象となっている、保護されたコンテンツまたはサービスのロックを解除するために使用される暗号化鍵マテリアルを含むこともできる。本発明による権利ラベルは、その権利ラベルが関連付けられているコンテンツまたはサービスに対して許可可能に発行される、すべてのライセンスの境界を定める定義を含む。従って、一般的に、ライセンスは、権利ラベルの中で規定された権利と条件のサブセットを含む。

#### 【0012】

本発明は、コンテンツの一部に対する権利記述および関連する保護された暗号化鍵マテリアルを受信すること、権利ラベルを生成するためにこのデータに対するデジタル署名の有効性を検査して生成すること、アプリケーションがコンテンツの一部に対するライセンスを要求するのを可能にすること、*DRM*ライセンシングサーバが上記要求に対する許可検

10

20

30

40

50

直を行うのを可能にすること、DRMライセンシングサーバが要求に基づいて要求側にライセンスを発行し、要求を行うアプリケーションまたはユーザに対するコンテンツの暗号化マテリアルを保護するのを可能にすることを含む機能を実行するプロトコルおよび／またはアプリケーションプログラムおよび／またはアプリケーションプログラムインタフェース（API）として実現することができる。

#### 【0013】

本発明の一実施形態では、デジタルコンテンツは、コンテンツをレンダリングすることを望んでいる1または複数のユーザに対応するデジタルライセンスを、ライセンスサーバが発行するのを可能にするために公表される。コンテンツは、コンテンツ鍵（CK）によって暗号化され、その結果として（CK（content））が得られ、コンテンツ鍵（CK）は、ライセンスサーバの公開鍵（PU-DRM）に従って保護され、コンテンツに関連する権利データは、（PU-DRM）に従って生成され、保護される。

10

#### 【0014】

保護された権利データと保護されたコンテンツ鍵（CK）は、ライセンスサーバによる署名を受けるために権利ラベルとしてライセンスサーバに提出される。ライセンスサーバは、権利ラベルの有効性を検査し、有効であれば、PU-DRMに対応する秘密鍵（PR-DRM）に基づいて、少なくともその一部が保護された権利データに基づいたデジタル署名を生成し、その結果として署名付き権利ラベル（SRL）が得られ、そのSRLが戻される。

#### 【0015】

戻されたSRLが受信されると、（CK（content））と連結されてコンテンツパッケージが形成され、このコンテンツパッケージは、1または複数のユーザに配信される。コンテンツをレンダリングすることを望むユーザは、コンテンツパッケージからSRLを取り出し、取り出したSRLをコンテンツに対応するライセンス要求の一部としてライセンスサーバに提出する。ライセンスサーバは、PU-DRMに基づいて、少なくともその一部が保護された権利データに基づいたSRLの署名を検査し、SRL内の保護された権利データにアクセスし、アクセスした権利データをレビューして、ユーザがライセンスを受ける権利があるか否かを判断し、権利があれば、ライセンスをユーザに発行する。ライセンスは、ユーザにアクセス可能な保護された形式で、CKを含んでいる。

20

#### 【0016】

#### 【発明の実施の形態】

本発明のその他の特徴は、添付図面を参照して以下に詳述する本発明の実施形態の説明の中で明らかにする。

30

#### 【0017】

#### （例示コンピューティングデバイス）

図1と以下の説明は、本発明を実現するのに適しているコンピューティング環境の概要を要約して説明することを目的としている。なお、当然に理解されるように、ハンドヘルド、ポータブル、およびあらゆる種類の他のコンピューティングデバイスが本発明に関連して使用されることが意図されている。以下では汎用コンピュータが説明されているが、これは単なる一例にすぎず、本発明が必要としているのは、ネットワークサーバが相互に動作可能で、対話可能なシンクライアント（thin client）だけである。従って、本発明を、クライアントリソースの実装をほとんど必要としないが、または最小限で済むようなネットワーク化されたホスト中心のサービスの環境、例えば、クライアントデバイスがワールドワイドウェブの単なるブラウザまたはインタフェースとして働くネットワーク化された環境で実現することができる。

40

#### 【0018】

必ずしもその必要はないが、本発明を、開発者によって使用されるようにアプリケーションプログラミングインタフェース（API）で実現すること、および／またはプログラムモジュールのように、クライアントワークステーション、サーバ、またはその他のデバイスなど1または複数のコンピュータによって実行されるコンピュータ実行可能命令とい

50

う広い文脈の中で、以下に説明されているネットワークブラウジングソフトウェアに含むこともできる。一般的に、プログラムモジュールは、特定のタスクを実行し、または特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。典型的には、プログラムモジュールの機能を、種々の実施形態での要求に応じて組み合わせたり、分散させたりすることができる。さらに、この当業者ならば理解されるように、本発明は、他のコンピュータシステム構成で実施することができる。本発明で使用するのに適している、他の周知コンピューティングシステム、環境および/または構成としては、これらに限定されないが、パーソナルコンピュータ（PC）、自動預金支払機、サーバコンピュータ、ハンドヘルドまたはラップトップデバイス、マルチプロセッサシステム、マイクロプロセッサベースのシステム、プログラム可能な家庭電化製品、ネットワークPC、ミニコンピュータ、メインフレームコンピュータなどがある。本発明は、タスクが通信ネットワークや他のデータ伝送媒体を通してリンクされているリモート処理デバイスによって実行されるような、分散型コンピューティング環境で実施することもできる。分散型コンピューティング環境では、プログラムモジュールを、メモリ記憶装置を含む、ローカルとリモートの両方のコンピュータ記憶媒体に配置することができる。

#### 【0019】

図1は、本発明を実現することができる適当なコンピューティングシステム環境100の例を示しているが、上記説明から明らかであるように、このコンピューティングシステム環境100は、適当なコンピューティング環境の単なる一例であり、本発明の使用または機能範囲を限定することを示唆するものではない。

また、このコンピューティング環境100は、例示動作環境100に示されているコンポーネントのいずれかが1つ、またはどのような組み合わせに関しても、依存関係や要求条件があることを意味するものでもない。

#### 【0020】

図1を参照して説明すると、本発明を実現するための例示システムは、コンピュータ110の形態をした汎用コンピューティングデバイスを含む。コンピュータ110のコンポーネントは、これらに限定されないが、処理ユニット120、システムメモリ130、およびシステムメモリを含む種々のシステムコンポーネントを処理ユニット120に結合しているシステムバス121がある。システムバス121は、数種類のバス構造のいずれかにすることができ、このようなバス構造としては、メモリバスやメモリコントローラ、ペリフェラルバス、および種々のバスアーキテクチャのいずれかを採用しているローカルバスがある。例を挙げると、このようなアーキテクチャは、これらに限定されないが、ISA（Industrial Standard Architecture）バス、MCA（Micro Channel Architecture）バス、EISA（Enhanced ISA）バス、VESA（Video Electronics Standards Association）ローカルバス、およびPCI（Peripheral Component Interconnect）バス（Mezzanineバスとも呼ばれている）がある。

#### 【0021】

コンピュータ110は、典型的には、種々のコンピュータ読取り可能媒体を装備しているのが代表的である。コンピュータ読取り可能媒体は、コンピュータ110によってアクセスできる媒体として利用可能なものであれば、どのような媒体にすることもでき、揮発性媒体と不揮発性媒体で、取り外し可能と取り外し不能の媒体が含まれている。例を挙げると、コンピュータ読取り可能媒体は、これらに限定されないが、コンピュータ記憶媒体と通信媒体がある。コンピュータ読取り可能媒体は、コンピュータ読取り可能命令、データ構造、プログラムモジュールまたは他のデータなどの、情報を格納するための方法または技術で実現された揮発性及び不揮発性、取り外し可能及び取り外し不能の媒体を含む。コンピュータ記憶媒体は、これらに限定されないが、RAM、ROM、EEPROM、フラッシュメモリや他のメモリ技術、CDROM、DVD（digital versatile

10

20

30

40

50

le disk) または他の光ディスクストレージ、磁気カセット、磁気テープ、磁気ディスクストレージや他の磁気記憶装置、または必要とする情報を格納するために使用することができ、コンピュータ110によってアクセス可能である他の媒体などを含む。通信媒体は、典型的には、コンピュータ読取り可能命令、データ構造、プログラムモジュールまたは他のデータを、搬送波や他の伝送機構などの変調されたデータ信号の形で具現化し、任意の情報配達媒体が含まれている。ここで「変調されたデータ信号」という用語は、信号中の情報を符号化するような方法で1または複数の特性が設定または変更されている信号を意味している。例を挙げると、通信媒体は、これらに限定されないが、ワイヤドネットワークまたはダイレクトワイヤド接続などのワイヤド媒体、および音響、RF、赤外線、および他のワイレス媒体などのワイヤレス媒体を含む。上述のどのような組み合わせも、コンピュータ読取り可能媒体の範囲に含まれる。

10

#### 【0022】

システムメモリ130は、ROM(read only memory)131、RAM(random access memory)132などのように、揮発性および/または不揮発性メモリの形体をしたコンピュータ記憶媒体を含む。スタートアップ時など、コンピュータ110内の要素間で情報を転送するのを支援する基本ルーチンから構成されたBIOS(basic input/output system)133は、典型的には、ROM131に格納されている。RAM132は、典型的には、即時に処理ユニット120によりアクセスされ、および/または処理されるデータおよび/またはプログラムモジュールを含む。例を挙げると、これらに限定されないが、図1は、オペレーティングシステム134、アプリケーションプログラム135、他のプログラムモジュール136、およびプログラムデータ137を示す。

20

#### 【0023】

コンピュータ110は、他の取り外し可能/取り外し不能、揮発性/不揮発性のコンピュータ記憶媒体を装備することもできる。単なる例示として、図1は、取り外し不能で不揮発性の磁気媒体との間で読み書きを行うハードディスクドライブ141、取り外し可能で不揮発性の磁気ディスク152との間で読み書きを行う磁気ディスクドライブ151、およびCDROMや他の光媒体などの、取り外し可能で不揮発性の光ディスク156との間で読み書きを行う光ディスクドライブ155を示す。例示動作環境で使用できる、他の取り外し可能/取り外し不能、揮発性/不揮発性のコンピュータ記憶媒体は、これらに限定されないが、磁気テープカセット、フラッシュメモ리카ード、DVD、デジタルビデオテープ、ソリッドステートRAM、ソリッドステートROMなどを含む。ハードディスクドライブ141は、典型的には、インタフェース140のような取り外し不能メモリインタフェースを介して、システムバス121に接続されている。磁気ディスクドライブ151と光ディスクドライブ155は、インタフェース150のような取り外し可能メモリインタフェースによりシステムメモリ121に接続されている。

30

#### 【0024】

上述した、図1に図示されたドライブとそれに関連するコンピュータ記憶媒体は、コンピュータ読取り可能命令、データ構造、プログラムモジュールおよび他のデータをコンピュータ110のために格納している。図1には、例えば、ハードディスクドライブ141は、オペレーティングシステム144、アプリケーションプログラム145、他のプログラムモジュール146、およびプログラム147を格納しているものとして示されている。なお、これらのコンポーネントは、オペレーティングシステム134、アプリケーションプログラム135、他のプログラムモジュール136、およびプログラムデータ137と同じであることもあれば、異なっていることもある。オペレーティングシステム144、アプリケーションプログラム145、他のプログラムモジュール146、およびプログラムデータ147が異なる番号になっているのは、これらが、最低限、異なるコピーであることを示すためである。ユーザは、キーボード162およびマウス、トラックボールまたはタッチパッドとも広く呼ばれているポインティングデバイス161などの入力デバイスを通して、命令と情報とをコンピュータ110に入力することができる。その他の入力デ

40

50

バイス（図示せず）は、マイクロホン、ジョイスティック、ゲームパッド、衛星アンテナ、スキャナなどを含む。これらおよび他の入力デバイスは、システムバス121に結合されているユーザ入力インタフェース160を通して、処理ユニット120に接続されているが、パラレルポート、ゲームポートまたはUSB（universal serial bus）などの他のインタフェースやバス構造で接続されていることもある。

#### 【0025】

モニタ191、他の種類の表示装置は、ビデオインタフェース190のようなインタフェースを介して、システムバス121に接続されている。Northbridgeなどのグラフィックスインタフェース182を、システムバス121に接続することができる。Northbridgeは、CPU、またはホストの処理ユニット120と通信し、AGP（accelerated graphics port）との通信を担当するチップセットである。1または複数のグラフィックス処理ユニット（GPU：graphics processor unit）184は、グラフィックスインタフェース182と通信することができる。この点に関して、GPU184は、一般的に、レジスタストレージのような、オンチップメモリストレージを含み、GPU184は、ビデオメモリ186とやりとりしている。なお、GPU184は、コプロセッサの単なる一例であり、種々のコプロセッサデバイスをコンピュータ110に含めることができる。モニタ191または他のタイフディスプレイデバイスは、ビデオインタフェース190のような、インタフェースを介してシステムバス121に接続され、インタフェースは、ビデオメモリ186と通信することができる。モニタ191のほかに、スピーカ197、プリンタ196などの、他の周辺出力装置をコンピュータに含むこともでき、これらの出力デバイスを、出力周辺インタフェース195を通して接続することができる。

#### 【0026】

コンピュータ110は、リモートコンピュータ180などの、1または複数のリモートコンピュータとの論理的コネクションを使用するネットワーク化された環境で動作することができる。リモートコンピュータ180は、パーソナルコンピュータ、サーバ、ルータ、ネットワークPC、ピアデバイスまたは他の共通ネットワークノードにすることができる。図1にはメモリ記憶装置181だけが示されているが、典型的には、コンピュータ110に関して上述した要素の多くまたはすべてを含む。図1に示した論理的コネクションは、LAN（local area network）171とWAN（wide area network）173とがあるが、他のネットワークを含めることもできる。このようなネットワーキング環境は、オフィス、企業内コンピュータネットワーク、イントラネットおよびインターネットとして普通になっている。

#### 【0027】

LANネットワーキング環境で使用されるときに、コンピュータ110は、ネットワークインタフェースまたはアダプタ170を通してLAN171に接続されている。WANネットワーキング環境で使用されるときに、コンピュータ110は、典型的には、インターネットなどのWAN173上の通信を確立するためのモデム172または他の手段を含む。モデム172は、内蔵型と外付け型があり、どちらも、ユーザ入力インタフェース160または他の適当な機構を介してシステムバス121に接続することができる。ネットワーキング環境では、コンピュータ110に関して上述したプログラムモジュールまたはその一部は、リモートのメモリ記憶装置に格納しておくことができる。図1は、単なる一例であり、これに限定されないが、リモートのアプリケーションプログラム185は、メモリデバイス181に置かれているものとして示されている。当然に理解されるように、図示のネットワークコネクションは単なる例であり、コンピュータ間の通信リンクを確立する他の手段を使用することもできる。

#### 【0028】

当業者ならば理解されるように、コンピュータ110または他のクライアントデバイスは、コンピュータネットワークの一部として配置することができる。この点に関して、本発明は、任意の数のメモリまたは記憶ユニットを有し、任意の数のアプリケーションとプロ

10

20

30

40

50

セスとが任意の数の記憶ユニットまたはボリュームにわたって実行されている、あらゆるコンピュータシステムにも関係する。本発明は、サーバコンピュータとクライアントコンピュータがネットワーク環境内に配置され、リモートまたはローカルのストレージを有している環境に適用することができる。本発明は、プログラミング言語機能、翻訳機能および実行機能を備えたスタンドアロン型コンピューティングデバイスにも適用できる。

#### 【0029】

分散型コンピューティングは、コンピューティングデバイスとシステム間で直接にやりとりすることにより、コンピュータリソースとサービスの共有を容易にする。これらのリソースとサービスは、情報をやりとりすること、キャッシュ記憶、およびファイルのディスク記憶を含む。分散型コンピューティングは、ネットワーク接続性を利用して、クライアントが集団の力を生かして企業全体に利益をもたらすことを可能にする。この点に関して、種々のデバイスは、トラステッドグラフィックスパイプライン（*trusted graphics pipeline*）に対する本発明の認証手法に関係するためによりやりとりをするアプリケーション、オブジェクトまたはリソースを有することができる。

#### 【0030】

図2は、例示のネットワーク化されたまたは分散型コンピューティング環境を示す概略図である。分散型コンピューティング環境は、コンピューティングオブジェクト10a、10bなど、およびコンピューティングオブジェクトまたはデバイス110a、110b、110cなどを含んでいる。これらのオブジェクトは、プログラム、メソッド、データストア、プログラマブルロジックなどを備える。オブジェクトは、PDA、テレビジョン、MP3プレーヤ、パーソナルコンピュータなどの同一または異なるデバイスの部分を備えることもできる。各オブジェクトは、通信ネットワーク14を介して他のオブジェクトと通信することができる。このネットワーク自体は、図2のシステムにサービスを提供する他のコンピューティングオブジェクトとコンピューティングデバイスとを含むことができる。本発明の一側面によれば、各オブジェクト10または110は、トラステッドグラフィックスパイプラインに対する本発明の認証手法を要求できるアプリケーションを含むことができる。

#### 【0031】

また、当然に理解されるように、110cのようなオブジェクトは、別のコンピューティングデバイス10または110上でホストとなることができる。従って、図示の物理的な環境は、接続されたデバイスがコンピュータとして示されているが、この図示は単なる例示であり、物理的な環境を、PDA、テレビジョン、MP3プレーヤなどの種々のデジタルデバイス、インタフェース、COMオブジェクトなどのソフトウェアオブジェクトを含むものとして、図示しまたは記載することもできる。

#### 【0032】

分散型コンピューティング環境をサポートするシステム、コンポーネント、およびネットワーク構成は、さまざまなものがある。例えば、コンピューティングシステムは、ワイヤライン（有線）またはワイヤレス（無線）システムによって、ローカルネットワークまたは広域分散型ネットワークによって接続される。現在では、ネットワークの多くがインターネットに結合され、インターネットが広域分散型コンピュータのインフラストラクチャを提供し、そこには多種類のネットワークが収容されている。

#### 【0033】

ホームネットワーキング環境では、少なくとも4種類のネットワーク伝送媒体があり、それらは、パワーライン、データ（ワイヤレスとワイヤドの両方）、音声（例えば、電話）およびエンターテインメントメディアなどの、独自のプロトコルをサポートすることができる。電灯スイッチ、家庭用電気器具などの大部分のホームコントロールデバイスは、パワーラインを使用して接続することができる。データサービスは、ブロードバンド（例えば、DSLまたはケーブルモデムのどちらか）として家庭に入ることができ、ワイヤレス（例えば、HomeRFまたは802.11b）またはワイヤド（例えば、HomePNA、Cat 5、普通の電源線）のどちらかから家庭内にアクセス可能である。音声トラフ

10

20

30

40

50

ィックは、ワイヤド（例えば、Cable 3）としても、ワイヤレス（例えば、セル電話）としても家庭に入ることができ、Cable 3ワイヤリングを使用して家庭内に配信することができる。エンターテインメントメディアは、衛星またはケーブルを通して家庭に入ることができ、典型的には、同軸ケーブルを使用して家庭内に配信される。IEEE 1394とDVIも、メディアデバイスのクラスタをデジタル相互接続するものとして出現している。

これらネットワーク環境およびプロトコル標準として出現するかもしれない他のネットワーク環境のすべては、イントラネットを構築するように相互接続することができ、イントラネットは、インターネットを通して外部世界と接続することができる。以上を要約すると、データを格納し、伝送するための様々な異なる種類のソースが存在し、その結果、今後の動向として、コンピューティングデバイスは、データ処理パイプラインのすべての部分でコンテンツを保護する方法が必要になる。

#### 【0034】

インターネットとは、コンピュータネットワーク分野では周知である、一組のTCP/IPプロトコルを利用するネットワークとゲートウェイとの集合と言われている。TCP/IPは、「Transport Control Protocol/Interface Protocol」を表す略語である。インターネットは、ユーザがネットワーク上で情報をやりとりし、共有することができるネットワークプロトコルを実行するコンピュータにより相互接続されている、地理的に分散されたリモートコンピュータネットワークとすることができる。情報共有がこのように広範囲にわたっているため、インターネットなどのリモートネットワークは、広くオープンシステムになるまで発達し、ここで、開発者は、特殊なオペレーションまたはサービスを実行するためのソフトウェアアプリケーションを、ほとんど制約なしで開発することができる。

#### 【0035】

従って、ネットワークインフラストラクチャは、クライアント/サーバ、ピアツーピア、またはハイブリッドアーキテクチャなどのネットワークトポロジのホストを可能にする。ここで「クライアント」は、あるクラスまたはグループのメンバーであり、そのクラスまたはグループとは関係のない別のクラスまたはグループのサービスを利用するものである。従って、コンピューティング分野では、クライアントは、別のプログラムから提供されるサービスを要求するプロセス、大雑把に言うと、命令またはタスクが集まったプロセスである。クライアントプロセスは、要求したサービスを利用するとき、他方のプログラムまたはサービス自体について動作の詳細を「知っている」必要はない。クライアント/サーバアーキテクチャにおいて、特に、ネットワーク化されたシステムでは、クライアントは、別のコンピュータ、例えばサーバによって提供される共有ネットワーク資源にアクセスするコンピュータである。図2の例では、コンピュータ110a、110bなどは、クライアントと考えることができ、コンピュータ10a、10bなどは、サーバと考えることができ、ここで、サーバ10a、10bは、クライアントコンピュータ110a、110bなどに複製されたデータを維持している。

#### 【0036】

サーバは、典型的には、インターネットなどのリモートネットワーク上でアクセス可能なリモートコンピュータシステムである。クライアントプロセスは、第1のコンピュータシステムでアクティブにしておくことができ、サーバプロセスは、第2のコンピュータシステムでアクティブにしておくことができ、通信媒体を通して相互に通信することにより、機能を分散させることができ、複数のクライアントがサーバの情報収集能力を利用することができる。

#### 【0037】

クライアントとサーバは、プロトコル層に提供されている機能を利用して相互に通信する。例えば、HTTP（Hypertext Transfer Protocol）は、ワールドワイドウェブ（WWW）に関連して使用される共通プロトコルである。典型的には、URL（Universal Resource Locator）またはIP（I

10

20

30

40

50

Internet Protocol) アドレスなどのコンピュータネットワークアドレスは、サーバコンピュータまたはクライアントコンピュータであることを相互に知らせるために使用される。ネットワークアドレスは、URLアドレスと呼ばれることもある。例えば、通信は、通信媒体上で行うことができる。具体的には、クライアントとサーバは、大容量通信のTCP/IPコネクションを通して相互に結合することができる。

#### 【0038】

従って、図2は、本発明を使用することができる例示のネットワーキングまたは分散型環境を示し、ここで、サーバは、ネットワーク/バスを通してクライアントコンピュータと通信している。より具体的には、複数のサーバ10a、10bなどは、LAN、WAN、イントラネット、インターネットなどとするところからなる通信ネットワーク/バス14を介して相互に接続され、ここには、ポータブルコンピュータ、ハンドヘルドコンピュータ、シンクライアント、ネットワーク化された家庭電気器具など、またはVCR、TV、オーブン、ライト、ヒータ、本発明にかかる他のデバイスなど複数のクライアントまたはリモートコンピューティングデバイス110a、110b、110c、110d、110eなどがある。従って、本発明は、信用されたソースからのセキュアコンテンツを処理し、格納し、またはレンダリングするときに望ましい、あらゆるコンピューティングデバイスにも適用することができる。

#### 【0039】

通信ネットワーク/バス14が、例えば、インターネットであるネットワーク環境において、サーバ10は、クライアント110a、110b、110c、110d、110eなどが、HTTPなどの、いくつかの公知プロトコルのいずれかで通信するWebサーバにすることができる。サーバ10は、分散型コンピューティング環境の特徴であるように、クライアント110となることもできる。

通信は、該当する場合には、ワイヤドにすることも、ワイヤレスにすることもできる。クライアントデバイス110は、通信ネットワーク/バス14を介して通信することもあれば、通信しないこともあり、また、独立の通信を関連付けることもできる。例えば、TVまたはVCRの場合には、その制御にはネットワーク化された側面がある場合と、ない場合とがある。各々のクライアントコンピュータ110とサーバコンピュータ10とは、種々のアプリケーションプログラムモジュールまたはオブジェクト135を備え付け、様々な種類の記憶要素またはオブジェクトへの接続またはアクセスを備えることができるので、これらにまたがってファイルを格納したり、またはファイルの部分をそこにダウンロードしまたは移動することができる。従って、本発明は、コンピュータネットワーク/バス14にアクセスして、やりとりすることができるクライアントコンピュータ110a、110bなどと、クライアントコンピュータ110a、110bなど、他のデバイス111およびデータベース20とやりとりすることができるサーバコンピュータ10a、10bなどとが置かれているコンピュータネットワーク環境で利用することができる。

#### 【0040】

(デジタル権利管理(DRM)の概要)

図13を参照して説明すると、デジタル権利管理(DRM)と実施とは、デジタルオーディオ、デジタルビデオ、デジタルテキスト、デジタルデータ、デジタルマルチメディアなどのデジタルコンテンツ12に関して高く望まれており、ここで、そのデジタルコンテンツ12は、ユーザに配信される。ユーザによって受信されると、そのユーザは、メディアプレーヤなどの適当なレンダリングデバイスを、パーソナルコンピュータ14などを使用して、そのデジタルコンテンツをレンダリングまたは「プレイ」する。

#### 【0041】

典型的には、このようなデジタルコンテンツ12を配信するコンテンツ所有者または開発者(以下、「所有者」と呼ぶ)は、配信されたデジタルコンテンツ12をユーザがどのように扱うかを制限することを望んでいる。例えば、コンテンツ所有者は、ユーザがそのコンテンツ12をコピーし、それを第2のユーザに再配信するのを制限したいと望む場合もある。配信されたデジタルコンテンツ12を、制限された回数だけ、ある時間だけ、あ

10

20

30

40

50



る装置の種類だけ、あるメディアプレーヤの種類だけ、あるユーザの種類だけプレイできるようにすることを望む場合がある。

#### 【0042】

しかし、配信が行われた後は、そのコンテンツ所有者は、デジタルコンテンツ12を制御できても、非常に限られている。DRMシステム10は、任意の形体のデジタルコンテンツ12のレンダリングまたはプレイを制御下で行うことができ、ここで、この制御を、フレキシブルにし、デジタルコンテンツのコンテンツ所有者によって定義することができる。典型的には、コンテンツ12は、任意の適当な配信チャネルを通してパッケージ13の形でユーザに配信される。配信されるデジタルコンテンツパッケージ13は、対称暗号化／平文化鍵(KD)(つまり、(KD(CONTENT)))を使用して暗号化されたデジタルコンテンツ12が、そのコンテンツ、そのコンテンツのライセンスを取得する方法などを示している他の情報とともに含まれている。

10

#### 【0043】

信用ベースのDRMシステムは、デジタルコンテンツ12の所有者が、そのデジタルコンテンツ12がユーザのコンピューティングデバイス14上でレンダリングされるのを許可される前に、満足しなければならないライセンスルールを指定することができる。このライセンスルールは、上述した時間的要件を含めておくこともでき、ユーザ／ユーザのコンピューティングデバイス14(以下、この用語は別段の断りがない限り、同じ意味で使用される)が、コンテンツ所有者またはその代理人から取得しなければならないデジタルライセンス16の中で具現化することもある。このライセンス16は、デジタルコンテンツを解読するための平文化鍵(KD)を含み、おそらくは、ユーザのコンピューティングデバイスによって解読可能な鍵に従って暗号化されている。

20

#### 【0044】

デジタルコンテンツ12の一部分のコンテンツ所有者は、ユーザのコンピューティングデバイス14が、ライセンス16の中でそのコンテンツ所有者により指定されたルールと要求条件に従うこと、つまり、ライセンス16内のルールと要求条件が満たされていなければ、デジタルコンテンツ12がレンダリングされないことを信用しなければならない。好ましくは、ユーザのコンピューティングデバイス14は、そのデジタルコンテンツ12に関連し、ユーザによって取得されたライセンス16に具現化されているライセンスルールに従う場合を除き、デジタルコンテンツ12をレンダリングすることがない信用されたコンポーネントまたは機構18を装備している。

30

#### 【0045】

信用されたコンポーネント18は、典型的には、ライセンス16が有効か否かを判断し、有効とされたライセンス16内のライセンスルールと要求条件をレビューし、レビューしたライセンスルールと要求条件に基づいて、要求側ユーザが、要求されたデジタルコンテンツ12を、要求された方法でレンダリングする権利を有しているか否かを、判断するライセンスエバリュエータ20を備えている。当然に理解されるように、ライセンスエバリュエータ20は、DRMシステム10で、デジタルコンテンツ12の所有者の要求を、ライセンス16内のルールと要求条件に従って履行するものと信用されており、ユーザは、悪意の有無に関係なく、あらゆる目的に信用されたエレメントを容易に変更することができないはずである。

40

#### 【0046】

当然に理解されるように、ライセンス16内のルールと要求条件は、ユーザがデジタルコンテンツ12をレンダリングする権利を有しているか否かを、ユーザはだれであるか、ユーザはどこにいるか、ユーザはどの種類のコンピューティングデバイスを使用しているか、どのレンダリングアプリケーションがDRMシステムをコールするのか、日付、時間などの、いくつかの因子に基づいて指定することができる。さらに、ライセンス16のルールと要求条件は、例えば、あらかじめ決めたプレイの回数、あらかじめ決めたプレイ時間にライセンス16を制限することもある。

#### 【0047】

50

ルールと要求条件を、任意の適当な言語とシンタックスに従ってライセンス16に指定することができる。例えば、言語は、満足しなければならない属性と値を指定するだけのこともあれば（例えば、DATE must be later than X）、特定のスクリプトに従って関数の実行を要求することもある（例えば、IF DATE > later than X, THEN DO. . . .）。

#### 【0048】

ライセンス16が有効であり、ユーザがライセンスのルールと要求条件を満足しているとライセンスエバリュエータ20が判断すると、デジタルコンテンツ12を、レンダリングすることができる。具体的には、コンテンツ12をレンダリングするには、平文化鍵（KD）がライセンス12から取得され、コンテンツパッケージ13からの（KD（CONTENT））に適用され、その結果として実際のコンテンツ12が得られ、その実際のコンテンツ12が実際にレンダリングされることになる。

#### 【0049】

（デジタルコンテンツの公表）

図3は、デジタルコンテンツを公表するための本発明にかかるシステムと方法の好適実施形態を示す機能ブロック図である。本明細書で用いられている「公表」という用語は、アプリケーションまたはサービスが、そのコンテンツに対してエンティティが発行できる権利と条件の集まりを、信用されたエンティティと共に設定し、その権利と条件をだれに発行できるかを設定するプロセスのことである。本発明によれば、公表プロセスは、デジタルコンテンツを暗号化し、コンテンツの作成者が可能な限りすべてのコンテンツユーザのために意図した永続的な実施可能権利のリストを関連付けることを含む。このプロセスを、コンテンツの作成者が意図している場合を除き、権利のいずれかへのアクセスまたはコンテンツへのアクセスを禁止するようにセキュアに実行することができる。

#### 【0050】

本発明の好適実施形態では、セキュアなデジタルコンテンツを公表するために、特に3つのエンティティを採用することができる。すなわち、クライアント300側で実行され、公表されるコンテンツを準備するコンテンツ準備アプリケーション302、クライアントデバイス300側に置かれているデジタル権利管理（DRM）アプリケーションプログラムインタフェース（API）306、および通信ネットワーク330を通して通信できるようにクライアント300に結合されているDRMサーバ320である。本発明の好適実施形態では、通信ネットワーク330は、インターネットを含むが、当然に理解されるように、通信ネットワーク330は、例えば、所有権のあるイントラネットなどのローカルまたは広域ネットワークにすることもできる。

#### 【0051】

コンテンツ準備アプリケーション302は、デジタルコンテンツを作成するあらゆるアプリケーションとすることができる。例えば、このアプリケーション302は、デジタルテキストファイル、デジタルミュージック、ビデオ、または他の類似コンテンツを作成するワードプロセッサ、他の出版者とすることができる。コンテンツは、例えば、ライブイベント、テープ記録されたイベントのストリーム化オーディオ／ビデオなど、ストリーム化されたコンテンツを含むこともできる。本発明によれば、コンテンツ準備アプリケーションは、ユーザが用意した鍵を使用して、そのユーザがコンテンツを暗号化することを奨励する。アプリケーション302は、その鍵を使用してデジタルコンテンツを暗号化し、その結果として暗号化デジタルファイル304を形成する。クライアントアプリケーションは、ユーザがデジタルコンテンツファイル304の権利データを用意することを奨励する。権利データは、デジタルコンテンツの権利を有する各エンティティのIDが含まれている。このエンティティは、例えば、個人、あるクラスの個人、またはデバイスにすることができる。各エンティティの権利データは、コンテンツ内にエンティティが有する権利のリストと、その権利の一部または全部に課されている条件とを含む。この権利は、デジタルコンテンツを読み取り、編集し、コピーし、印刷するなどの権利を含むことができる。さらに、権利は、包含的にも、排他的にもすることができる。包含的権利は、特定のユー

10

20

30

40

50

サがコンテンツに特定の権利を有することを示している（例えば、ユーザはデジタルコンテンツを編集することができる）。排他的権利は、特定のユーザが特定の権利を除き、コンテンツにすべての権利を有することを示している（例えば、ユーザはコピーすること以外は、デジタルコンテンツに対して何でも行うことができる）。

#### 【0052】

本発明の一実施形態によれば、クライアントAPI306は、暗号化デジタルコンテンツと権利データをDRMサーバ320に渡すことができる。以下に詳しく説明されているプロセスを使用して、DRMサーバ320は、ユーザが割り当てた権利を実施できるかどうかを判断し、そうであれば、DRMサーバ320は権利データに署名し、署名付き権利ラベル(SRL)308を形成する。なお、一般的には、信用されたエンティティは、好ましくはDRMサーバ320により信用された鍵を使用して、権利データに署名することができる。例えば、クライアントは、DRMサーバ320から与えられた鍵を使用して権利データに署名することができる。

#### 【0053】

権利ラベル308は、権利の記述を表わすデータ、暗号化コンテンツ鍵、および権利記述と暗号化コンテンツ鍵に対するデジタル署名とを含むことができる。

DRMサーバが権利ラベルに署名する場合には、DRMサーバは、署名付き権利ラベル308をクライアントAPI306経由でクライアントに送り返し、署名付き権利ラベル308をクライアントデバイス300に格納する。コンテンツ準備アプリケーション302は、署名付き権利ラベル308を暗号化デジタルコンテンツファイル304と関連付ける。例えば、SRL308を、暗号化デジタルコンテンツファイルと連結し、権利管理コンテンツファイル310を生成する。

なお、一般的には、権利データは、デジタルコンテンツと結合する必要はない。

例えば、権利データを、既知のロケーションに格納しておくことができ、格納された権利データのレファレンスを、暗号化デジタルコンテンツと結合することができる。このレファレンスは、権利データがどこに格納されているかを示す識別子（例えば、権利データを含むデータストア）、およびその特定のストレージのロケーションに置かれている、その特定の権利データに対応する識別子（例えば、関心のある特定の権利データが置かれているファイルを特定するもの）を含むことができる。権利管理コンテンツ310は、どこにいてもだれにでも配信することができ、コンテンツを消費する権利を有するエンティティだけが、コンテンツを消費することができ、しかも、そのエンティティに割り当てられた権利に従ってのみコンテンツを消費することができる。

#### 【0054】

図4は、権利管理デジタルコンテンツを公表するための本発明による例示方法400を示すフローチャートであり、ここで、権利ラベルは、DRMサーバによって署名されている。なお、当然に理解されるように、この実施形態は、単なる例示であり、権利ラベルを、一般的には、あらゆる信用されたエンティティによって署名することができる。一般的には、デジタルコンテンツを公表するための本発明による方法は、コンテンツ鍵(CK)を使用してデジタルコンテンツを暗号化し、デジタルコンテンツに関連する権利記述を生成し、DRMサーバの公開鍵(PU-DRM)に従ってコンテンツ鍵(CK)を暗号化して、その結果として(PU-DRM(CK))が得られるようにし、権利記述と(PU-DRM(CK))との結合に対して(PU-DRM)に対応する秘密鍵(PR-DRM)に基づいて、デジタル署名を生成することを含むことができる。

#### 【0055】

ステップ402において、アプリケーション302は、デジタルコンテンツを暗号化するために使用されるコンテンツ鍵(CK)を生成する。好ましくは、コンテンツ鍵(CK)は対称鍵になっているが、一般的には、どの鍵を使用してもデジタルコンテンツを暗号化することができる。対称鍵アルゴリズムは、「秘密鍵」アルゴリズムと呼ばれることもあるが、メッセージを暗号化するときに使用した同じ鍵を使用して、メッセージを解読する。そのような理由から、(CK)は秘密に保っていることが好ましい。送信側と受信側の

10

20

30

40

50

間で (CK) を共有することは、(CK) が無許可でインターセプトされるのを防止するために、慎重に行う必要がある。(CK) は、暗号化する側と解読する側の両方で共有されるので、(CK) は、好ましくは、暗号化されたメッセージが送信される前に通知される。

#### 【0056】

この分野では、いくつかの対称鍵生成アルゴリズムがよく知られている。好適実施形態では、DES (Data Encryption Standard) が採用されるが、当然に理解されるように、他の対称鍵アルゴリズムも使用することができる。このような対称鍵アルゴリズムの例を挙げると、これらに限定されないが、Triple-DES、IDEA (the International Data Encryption Algorithm)、CAST、CAST-128、RC4、RC5、Skipjack がある。

#### 【0057】

ステップ404において、アプリケーション302は、対称コンテンツ鍵 (CK) を使用してデジタルコンテンツを暗号化し、暗号化デジタルコンテンツ304を形成する。これは、(CK (content)) という表記を使用して書かれている。アプリケーション302を使用する作成者は、デジタルコンテンツに関連する権利データを生成することもできる。権利データは、コンテンツを消費する権利があるエンティティのリストと、コンテンツに対してエンティティの各々が所有している特定の権利とを、その権利に課されている条件とともに含むことができる。この権利は、例えば、コンテンツを表示すること、コンテンツを印刷することなどを含むことができる。アプリケーション302は、権利データを API 306 に渡す。XML/XHTML フォーマットの権利データの例は、付録1として本明細書に添付されている。

#### 【0058】

ステップ406において、API 306 は、第2の暗号化鍵 (DES1) を生成する。これは、コンテンツ鍵 (CK) を暗号化するために使用される。好ましくは、(DES1) は対称鍵である。ステップ408において、API 306 は、(DES1) を使用して (CK) を暗号化し、その結果として (DES1 (CK)) を得る。ステップ410において、API 306 は (CK) を破棄するので、(CK) は、(DES1 (CK)) を解読することによってのみ取得できるようになる。(CK (content)) が中央の DRM サーバ320に対して保護されること、およびコンテンツに対するすべての「ライセンス要求」が権利データに従って行われることを保証するために、API 306 は、ステップ412において、用意されている DRM サーバ320に連絡し、公開鍵 (PU-DRM) を取り出す。ステップ414において、API 306 は、(PU-DRM) を使用して (DES1) を暗号化し、その結果として (PU-DRM (DES1)) を得る。従って、(CK) は、(PU-DRM) に対して保護され、(CK (content)) を解読する必要が起ったとき、DRM サーバ320が (CK) にアクセスできる唯一のエンティティとなることを保証することができる。ステップ416において、API 306 は、(DES1) を使用して権利データ (つまり、許可されたエンティティのリストと、リスト内の許可された各エンティティに関連する権利と条件) を暗号化し、その結果として (DES1 (rights data)) を得る。

#### 【0059】

別の実施形態では、(CK) を使用して、権利データを直接に暗号化し、その結果として (CK (rights data)) を得るので、(DES1) の使用を完全に無くすることができる。しかし、権利データを暗号化するために (DES1) を使用すると、DRM サーバに従う特定のアルゴリズムに、その (DES1) を適合させることが可能になるが、他方、(CK) は、DRM サーバから独立したエンティティによって指定され、DRM サーバに準拠しないことになる。

#### 【0060】

ステップ418において、コンテンツ保護アプリケーション302は、署名のための権利

10

20

30

40

50

ラベルとして、(PU-DRM(DES1))と(DES1(ハッシュ値))とをDRMサーバに提出することができる。別の方法として、クライアント自身が、権利データに署名することもできる。権利データが署名のためにサーバに提出される場合には、ステップ420において、DRMサーバ320は、権利データにアクセスし、提出された権利ラベル内の権利と条件を実施できることを確認する。権利データを実施できることを確認するために、DRMサーバ320は、(PR-DRM)を(PU-DRM(DES1))に適用し、その結果として(DES1)を得て、(DES1)を(DES1(ハッシュ値))に適用し、その結果として平文の権利データを得る。次に、サーバ320は、いずれかのポリシチェックを行って、権利データに指定されているユーザ、権利、および条件がサーバ320によって実施されたポリシの範囲内にあることを確かめることができる。サーバ320は、(PU-DRM(DES1))と(DES1(ハッシュ値))とを含んでいる、最初に提出された権利データに署名し、その結果として署名付き権利ラベル(SRL)308を得る。ここで、署名は、DRMサーバ320の秘密鍵(PR-DRM)に基づいており、SRL308をAPI306に送り返し、戻されたSRL308をクライアントアプリケーション302に提示する。

#### 【0061】

SRL308は、デジタル署名されたドキュメントであり、不正行為に強くなっている。さらに、SRL308は、コンテンツを暗号化するために使用された実際の鍵のタイプとアルゴリズムから独立しているが、SRL308が保護しているコンテンツと強い1対1の関係を保っている。図5に示すように、本発明の一実施形態では、SRL308は、おそらくコンテンツのIDを含む、SRL308の基礎となっているコンテンツに関する情報と、(PU-DRM(DES1))を含む、SRL308に署名したDRMサーバに関する情報と、ネットワーク上のDRMサーバを見つけるためのURLなどの照会情報、およびURLが失敗したときのフォールバック情報と、SRL308自体を記述している情報と、(DES1(ハッシュ値)):(DES1(CK))と、S(PR-DRM)とを含むことができる。XML/XrMLにおけるSRL308の例は、付録2として本明細書に添付されている。

#### 【0062】

信用されたエンティティは、権利データに署名して、署名付き権利ラベル308を生成することを確認することによって、DRMサーバは、権利ラベル308の権利データに記述されているように出版者によって規定された項目に従って、コンテンツに対するライセンスを発行することを主張する。当然に理解されるように、ユーザは、特にライセンスがコンテンツ鍵(CK)を含んでいるために、コンテンツをレンダリングするためのライセンスを取得することが要求される。ユーザが暗号化コンテンツに対するライセンスを取得したいときには、ユーザは、コンテンツに対するSRL308と、ユーザの信用証明物を検証する証明書を含むライセンス要求を、DRMサーバ320または他のライセンス発行エンティティに提示することができる。ライセンス発行エンティティは、(PU-DRM(DES1))と(DES1(ハッシュ値))とを解読し、権利データを生成して、作成者(存在する場合)によってライセンス発行エンティティに許可されたすべての権利をリストし、その特定権利だけを含むライセンスを構築することができる。

#### 【0063】

好ましくは、アプリケーション302がSRL308を受け取ると、そのアプリケーション302は、署名付き権利ラベル308を対応する(CK(コンテンツ))304と連結し、権利管理デジタルコンテンツを形成する。別の方法として、権利データを、暗号化デジタルコンテンツが提供されているロケーションのレファレンスとともに、そのロケーションに格納することができる。従って、DRM対応のレンダリングアプリケーションは、そのレンダリングアプリケーションがレンダリングしようとしているコンテンツ部分を通して、署名付き権利ラベル308を見つけることができる。署名付き権利ラベルが見つかると、レンダリングアプリケーションをトリガし、DRMサーバ320に対してライ

10

20

30

40

50

センス要求を開始する。公表アプリケーション 302 は、例えば、DRM ライセンスサーバ 320 に URL を格納することができ、DRM ライセンスサーバは、権利ラベルにデジタル署名する前に、自身の URL をメタデータの一部として権利ラベルに組み込むことができ、レンダリングアプリケーションによってコールされた DRM クライアント API 306 は、正しい DRM ライセンスサーバ 320 を特定することができる。好ましくは、例えば、GUID (globally unique identifier) などのユニーク識別子は、その署名の前に権利ラベルに組み入れられている。

#### 【0064】

本発明の好適実施形態では、SOAP (Simple object access protocol) を使用して、コンテンツ保護アプリケーション 302 またはレンダリングアプリケーションと DRM サーバ 320 との間の通信を行うことができる。さらに、API 306 などの API ライブラリを用意しておけば、アプリケーション 302 などのアプリケーションは、DRM プロトコルのクライアント側に実装する必要がなくなり、ローカル API コールを行うだけで済むようになる。好ましくは、XML、XML 言語を使用して、権利記述、ライセンス、およびデジタルコンテンツの権利ラベルを記述するが、当然に理解されるように、適当なフォーマットを、権利記述と他のデータに使用することができる。

#### 【0065】

(公表されるコンテンツのライセンスの取得)

図 6 は、権利管理デジタルコンテンツをライセンスングするための本発明にかかるシステムと方法の好適実施形態を示す機能ブロック図である。本明細書で用いられている「ライセンスング」という用語は、ライセンスの中で指名されたエンティティが、ライセンスに規定された条項に従ってコンテンツを消費するのを可能にするライセンスを要求し、および受け取るために、アプリケーションまたはサービスが従うプロセスのことである。ライセンスプロセスへの入力は、ライセンスを要求されたコンテンツに関連する署名付き権利ラベル (SRL) 308、およびライセンスを要求されたエンティティの公開鍵証明書を含むことができる。当然に理解されるように、ライセンスを要求するエンティティは、必ずしも、ライセンスを要求されたエンティティである必要はない。典型的には、ライセンスは、SRL 308 からの権利記述、暗号化コンテンツを解読できる暗号化鍵、および権利記述と暗号化鍵に対するデジタル署名を含む。デジタル署名は、指名されたエンティティと権利が合法的であることを示している。

#### 【0066】

アプリケーション 302 が権利管理コンテンツ 310 を消費する 1 つの方法は、クライアント API 306 が、権利管理コンテンツ 310 の署名付き権利ラベル 308 を、通信ネットワーク 330 を介して DRM サーバ 320 に転送することである。DRM サーバ 320 が置かれているロケーションは、例えば、SRL 308 の照会情報の中に見つけることができる。このような実施形態では、DRM ライセンシングサーバ 320 は、以下に詳しく説明されているプロセスを通して、権利ラベルの中の権利記述を使用してライセンスを発行できるか否かを判断し、そうであれば、ライセンスに含まれる権利記述を取り出すことができる。上述したように、権利ラベル 308 は、DRM サーバ 320 の公開鍵 (PU-DRM) に従って暗号化されたコンテンツ鍵 (CK) (すなわち、(PU-DRM (CK))) を含む。ライセンスを発行するプロセスにおいて、DRM サーバ 320 は、この値をセキユアに解読して (CK) を取得する。そのあと、ライセンス要求において渡された公開鍵証明書の公開鍵 (PU-ENTITY) を使用して、(CK) を再暗号化する (すなわち、(PU-ENTITY (CK)))。新たに再暗号化された (PU-ENTITY (CK)) は、サーバ 320 がライセンスに入れるものである。従って、ライセンスを、関連する秘密鍵 (PR-ENTITY) の所持者だけが (PU-ENTITY (CK)) から (CK) を回復できるので、(CK) が公表されるリスクなしに、コール側に戻すことができる。次に、クライアント API 306 は (CK) を使用して、暗号化コンテンツを解読し、解読されたデジタルコンテンツ 312 を形成する。クライアントアプリケ

10

20

30

40

50

ーション 302 は、ライセンスに提供されている権利に従って、解読されたデジタルコンテンツ 312 を使用することができる。

【0067】

別の方法として、例えば、公表クライアントなどのクライアントは、コンテンツを消費するために独自のライセンスを発行することもできる。このような実施形態では、セキュアされたプロセスを、適当な状況の下でデジタルコンテンツを解読するために必要な鍵をクライアントに提供するクライアントコンピュータ上で実行することができる。

【0068】

図 7 と図 8 は、権利管理デジタルコンテンツをライセンシングするための本発明によるシステムと方法の好適実施形態のフローチャートを示す図である。本発明によれば、要求側のエンティティは、1 または複数の潜在的ライセンスに代わってライセンス要求を提出することができる。潜在的ライセンスとしては、人、グループ、デバイス、またはなんらかの方法でコンテンツを消費できる他のエンティティなどがある。以下に説明する方法 600 の実施形態では、DRM サーバがライセンス要求を処理するようになっているが、当然に理解されるように、ライセンス要求処理をクライアント側で行い、ライセンスをクライアントに直接に発行させることもできる。

【0069】

ステップ 602 において、例えば、DRM サーバなどのライセンス発行エンティティは、ライセンス要求を受け取る。好ましくは、ライセンス要求は、1 または複数の要求されたライセンスの各々の公開鍵証明書または ID のどちらかを含む。以下に、ライセンス要求の好適実施形態の SOAP フロトコルを示す。

【0070】

【表 1】

```
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <AcquireLicense xmlns="http://xxxx.com/PublishingService">
      <RequestParams>
        <AcquireLicenseParams>
          <LicenseeCerts>
            <String>string</String>
            <String>string</String>
          </LicenseeCerts>
          <RightsSpecification>string</RightsSpecification>
          <RightsOfferID>string</RightsOfferID>
          <ApplicationData>string</ApplicationData>
        </AcquireLicenseParams>
        <AcquireLicenseParams>
          ...
        </AcquireLicenseParams>
      </RequestParams>
    </AcquireLicense>
  </soap:Body>
</soap:Envelope>
```

【0071】

ステップ 604 において、要求側のエンティティ（すなわち、ライセンス要求を行うエンティティ）が認証される。本発明の一実施形態によれば、ライセンス発行エンティティを、フロトコル（例えば、チャレンジャー応答）認証を使用して、要求側エンティティの ID を判断するように構成することも、要求側エンティティの認証を要求しないように（これ

10

20

30

40

50

は、「匿名認証を許容する」とも呼ばれる）構成することもできる。認証が要求される場合には、あらゆる種類の認証方式を使用することができ（例えば、上述のチャレンジ応答方式、MICROSOFT.NET、PASSPORT、WINDOWS（登録商標）authentication、X509などのユーザID・パスワード方式）。好ましくは、匿名認証が許容されるとともに、統合された情報システムによってサポートされる、あらゆるプロトコル認証方式をサポートする。認証ステップの結果は、例えば、「匿名」ID（匿名認証の場合）などのIDであるか、またはパーソナルアカウントIDである。ラインセンス要求がなんらかの理由で認証できないときは、エラーが戻され、ラインセンスは許可されない。

【0072】

ステップ606において、認証されたエンティティが許可される。つまり、ステップ608で認証されたエンティティが、ライセンスを要求するのを許されているか否か（自身のためか、別のエンティティのためか）が判断される。好ましくは、ライセンス発行エンティティは、ライセンスを要求するのを許されている（または許されていない）エンティティのリストを格納する。好適実施形態では、このIDリストの中のIDは、ライセンスが要求されるエンティティのIDではなく、要求を行うエンティティのIDになっているが、どちらにすることも可能である。例えば、パーソナルアカウントIDは、ライセンス要求を直接に行うことが許されていないが、トラステッドサーバプロセスは、そのエンティティに代行してライセンス要求を行うことができる。

【0073】

本発明によれば、ライセンス要求には、各潜在的ライセンスの公開鍵証明書またはIDのどちらも含むことができる。ライセンスが1人のライセンスのためにだけ要求されるときは、1つの証明書またはIDだけが指名される。ライセンスが複数のライセンスのために要求されるときは、証明書またはIDは、各潜在的ライセンスに対して指名される。

【0074】

好ましくは、ライセンス発行エンティティは、有効なライセンスごとに公開鍵証明書を持っている。しかし、アプリケーション302は、所与のユーザにライセンスを生成することを望む場合でも、アプリケーション302は、そのユーザの公開鍵証明書にアクセスできないことがある。このような場合は、アプリケーション302は、ライセンス要求の中でユーザのIDを指定できるので、その結果、ラインセンス発行エンティティは、ディレクトリサービスのルックアップを実行して、該当ユーザの公開鍵証明書を戻す登録された証明書のプラグインモジュールを呼び出すことができる。

【0075】

ステップ608において、発行エンティティがライセンス要求に公開鍵証明書が含まれていないと判断したときは、発行エンティティは、指定されたIDを使用して、ディレクトリサービスまたはデータベースのルックアップを実行して、該当する公開鍵証明書を探し出す。ステップ610において、発行エンティティは、証明書がディレクトリにあると判断したときは、ステップ612で、その証明書が取り出される。好適実施形態では、証明書プラグインを使用して、ディレクトリアクセスプロトコルを介して、ディレクトリサービスから公開鍵証明書を取り出す。所与の潜在的ライセンスの証明書を、要求またはディレクトリの中に見つけることができないときには、ライセンスサーバは、その潜在的ライセンスのライセンスを生成しないので、ステップ614において、エラーを要求側エンティティに戻す。

【0076】

ライセンス発行エンティティが、少なくとも1つの潜在的ライセンスの公開鍵証明書を有すると、ステップ616において、発行エンティティは、ライセンス証明書の信頼性を検証する。好ましくは、発行エンティティは、1組の信用された証明書発行者証明書を有するように構成され、ライセンス証明書の発行者が、信用された発行者のリストにあるか否かを判断する。ステップ616において、発行エンティティは、ライセンス証明書の発行者がトラステッド発行者のリストにないとは判断したときには、そのライセンスに対する要

10

20

30

40

50



求は失敗し、ステップ614においてエラーが生成される。従って、信用された発行者によって発行されていない証明書を持つ潜在的ライセンスは、ライセンスを受け取らない。

#### 【0077】

さらに、発行エンティティは、好ましくは、信用された発行者証明書から個別のライセンスの公開鍵証明書までに至る証明書チェーンの中のすべてのエンティティに対してデジタル署名の有効性検査を実行する。チェーンの中のデジタル署名の有効性を検査するプロセスは、周知のアルゴリズムである。所与の潜在的ライセンスに対する公開鍵証明書が有効でないとき、またはチェーンの中の証明書が有効でないときには、潜在的ライセンスは信用されないため、ライセンスをその潜在的ライセンスに発行しない。そうでなければ、ステップ618において、ライセンスを発行する。このプロセスは、ライセンスが要求されているすべてのエンティティが処理されるまで、ステップ620から繰り返される。

#### 【0078】

図8に示すように、ライセンス発行エンティティは、ライセンス要求の中で受け取られた署名付き権利ラベル308の有効性検査に進む。好適実施形態では、発行エンティティは、権利ラベルフラグインとバックエンドデータベースを使用して、発行エンティティによって署名されたすべての権利ラベルのマスタコピーを、サーバに苦悩することができ、権利ラベルは、公表時に権利ラベルに入れられたGUIDで識別される。ライセンス時に（ステップ622）、発行エンティティは、ライセンス要求の中の権利ラベル入力を解析し、そのGUIDを取り出す。このGUID、権利ラベルフラグインに渡され、そこからデータベースに対するクエリが出され、マスタ権利ラベルのコピーが取り出される。マスタ権利ラベルは、ライセンス要求の中で送信された権利ラベルのコピーよりも最新であるので、以下のステップでは、これが要求の中で使用される権利ラベルとなる。権利ラベルがGUIDに基づいてデータベースに見つからないときには、発行エンティティは、ステップ624においてそのポリシーをチェックし、要求の中の権利ラベルに基づいてライセンスを発行することがまだ許されているかを判断する。ポリシーがこれを許していなければ、ライセンス要求は、ステップ626において失敗し、ステップ628において、エラーがAPI306に戻される。

#### 【0079】

ステップ630において、ライセンス発行エンティティは、権利ラベル308の有効性を検査する。権利ラベル上のデジタル署名が有効性検査され、ライセンス発行エンティティが権利ラベルの発行者（権利ラベルに署名したエンティティ）でなければ、ライセンス発行エンティティは、権利ラベルの発行者が別の信用されたエンティティ（つまり、鍵マテリアルをライセンス発行エンティティと共有できるエンティティ）であるかを判断する。権利ラベルが有効でないか、または権利ラベルが信用されたエンティティによって発行されたものでなければ、ライセンス要求は、ステップ626において失敗し、ステップ628において、エラーがAPI306に戻される。

#### 【0080】

すべての有効性検査が行われた後、ライセンス発行エンティティは、承認されたライセンスの各々に対して権利ラベル308をライセンスに変換する。ステップ632において、ライセンス発行エンティティは、各ライセンスに対して発行されるライセンスに関するそれぞれの権利記述を生成する。各ライセンスについて、発行エンティティは、そのライセンスの公開鍵証明書に指名されているIDを、権利ラベルの中の権利記述に指名されているIDと突き合わせて評価する。

権利記述は、ライセンスの権利または権利セットを行使できるIDセットを、すべての権利または権利セットに割り当てる。このライセンスのIDが関連付けられているすべての権利または権利セットについて、その権利または権利セットは、ライセンスの新しいデータ構造の中にコピーされる。その結果のデータ構造は、特定のライセンスのライセンスにおける権利記述である。このプロセスの一部として、ライセンス発行エンティティは、権利ラベルの権利記述における権利または権利セットのいずれかと関連付けられている前提

10

20

30

40

50

条件を評価する。例えば、権利は、時間に関する時間前提条件が関連付けられていること  
があり、これは、指定した時間が経過した後、ライセンス発行エンティティがライセンス  
を発行するのを制限する。この場合には、発行エンティティは、現在の時間をチェックす  
る必要があり、その時間が、前提条件の中で指定された時間を経過していれば、発行エン  
ティティは、そのライセンスのIDがその権利と関連付けられていた場合でも、ライセン  
シに対してその権利を発行することができなくなる。

【0081】

ステップ636において、発行エンティティは、権利ラベルから(PU-DRM(DES  
1))と(DES1(CK))を取り出し、(PR-DRM)を適用して(CK)を得る

10

次に、発行エンティティは、ライセンスの公開鍵証明書(PU-ENTITY)を使用し  
て(CK)を再暗号化し、その結果として(PU-ENTITY(CK))を得る。

ステップ638において、発行エンティティは、生成された権利記述を(PU-ENT I  
TY(CK))と連結し、(PR-DRM)を使用してその結果のデータ構造にデジタル  
署名する。この署名付きデータ構造は、この特定ライセンスのライセンスである。

【0082】

ステップ640において、発行エンティティが、特定要求に対して生成すべきライセンス  
が残っていないと判断したときには、ゼロまたはそれ以上のライセンスを生成したことにな  
る。生成されたライセンスは、そのライセンスと関連付けられた証明書チェーン(例え  
ば、サーバの独自の公開鍵証明書のほか、その証明書を発行した証明書など)とともに

20

、ステップ642において要求側エンティティに戻される。

【0083】

以下に、ライセンス応答の好適実施形態のSOAPプロトコルを示す。

【0084】

【表2】

```
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <AcquireLicenseResponse xmlns="http://xxxx.com/LicensingService">
      <AcquireLicenseResult>
        <AcquireLicenseResponse>
          <CertificateChain>
            <String>string</String>
            <String>string</String>
          </CertificateChain>
        </AcquireLicenseResponse>
        <AcquireLicenseResponse>
          ...
        </AcquireLicenseResponse>
        ...
      </AcquireLicenseResult>
    </AcquireLicenseResponse>
  </soap:Body>
</soap:Envelope>
```

30

40

【0085】

本発明によるシステムの好適実施形態では、複数のライセンス鍵を使用することができ  
る。このような実施形態では、暗号化されて権利ラベル308を介してライセンスに移され  
るコンテンツ鍵(CK)は、実際には、どのような任意データにもすることができ。特

50

に有用な方法の１つは、それぞれが権利記述の中の異なる権利または異なる本人と関連付けられている、複数の別々に暗号化されたコンテンツ鍵（ＣＫ）を使用することである。例えば、アルバム上の歌曲のデジタル版は、すべてを異なる鍵（ＣＫ）で暗号化される。これら鍵（ＣＫ）は、同じ権利ラベルに含まれるが、本人は歌曲の１つをプレイする権利を有することができる（例えば、本人は、自分のライセンスの１つの鍵を取得する権利だけを有することができる）、別の人は、すべての歌曲をプレイする権利を有することができる（自分のライセンスのすべての鍵を取得する権利を有することになる）。

#### 【００８６】

好ましくは、本発明にかかるシステムは、公表アプリケーション／ユーザが、権利ラベル 308 のライセンスのグループまたはクラスを指名することを可能にする。このような実施形態では、ライセンス発行エンティティは、権利ラベルの中で指名されたグループ／クラスを評価して、現在のライセンスＩＤが、そのグループ／クラスのメンバーであるか否かを判断する。指名されたグループ／クラスのメンバーであると判断されると、発行エンティティは、そのグループ／クラスに関連する権利または権利のセットを、ライセンスのために使用される権利記述データ構造に追加することができる。

#### 【００８７】

本発明の好適実施形態では、ＤＲＭサーバの公表およびライセンスプロトコルインタフェースは、コール側アプリケーションまたはユーザの認証と許可をサポートしている。ＤＲＭサーバの管理コンソールは、アドミニストレータが、ライセンシングと公表の両方のインタフェースに対するアクセス制御リストを生成できるようにする。このようにすると、サーバの顧客は、ユーザ／アプリケーションが、公表またはライセンス、またはその両方を行うことを許容するポリシーを適用することができる。

#### 【００８８】

（署名付き権利ラベルの修正または再公表）

本発明の一実施形態では、コンテンツのユーザが、そのようなことを行う十分な許可が与えられていれば、ＳＲＬ 308 を「再公表」することができる。すなわち、そうすることが許されていれば、ユーザは、ＳＲＬ 308 内の権利データを変更することができる。特に、このような権利データを変更する許可を、権利データを変更する許可を有するユーザが、本質的に、関連するコンテンツに対してその広範な権利を許可することができるように、控え目に、賢明に行うべきである。考えられることは、このようなユーザは、コンテンツを公表し、それを外部に転送する権利を自身に許可することができる。

#### 【００８９】

ここでは、変更する許可は、特定のユーザまたはユーザのクラスが権利データと権利ラベル 308 とを実際に変更し、または「再公表」できるとの指示を、ＳＲＬ 308 内の権利データに含めることによって通知される。ＤＲＭサーバ 320 は、ライセンスの要求に関連してこのような許可を有するＳＲＬ 308 を受け取ると、ＤＲＭサーバ 320 は、ユーザの公開鍵（つまり、ＰＵ－ＥＮＴＩＴＹ）に従って暗号化されたユーザの対称鍵（ＤＥＳ１）が、結果として（ＰＵ－ＥＮＴＩＴＹ（ＤＥＳ１））となる、要求されたライセンスに含める。

#### 【００９０】

従って、ＳＲＬ 308 内の権利データを編集するには、図 9 に示すように、ユーザは、ライセンスから（ＰＵ－ＥＮＴＩＴＹ（ＤＥＳ１））を取り出し（ステップ 701）、（ＰＲ－ＥＮＴＩＴＹ）をそれに適用し、その結果として（ＤＥＳ１）を得るようにし（ステップ 703）、ＳＲＬ 308 から（ＤＥＳ１（ｒｉｇｈｔｓ ｄａｔａ））を取り出し（ステップ 705）、（ＤＥＳ１）をそれに適用し、その結果として権利データを得る（ステップ 707）。そのあと、ユーザは、希望通りに権利データを変更し（ステップ 709）、変更された権利データを、図 4 を参照して説明した方法で ＤＲＭ 320 に提出し、署名付き権利ラベル 308 を得る（ステップ 711）。もちろん、ここでは、署名付き権利ラベル 308 は、実際には再公表された ＳＲＬ 308 であり、ＳＲＬ 308 が受け取られた後（ステップ 713）、ユーザは、関連するコンテンツに連結されていた元の ＳＲＬ 30

10

20

30

40

50

8を取り除き（ステップ715）、その再公表されたSRL308を、そのコンテンツに連結する（ステップ717）。

#### 【0091】

以上から当然に理解されるように、SRL308を再公表すると、ユーザは、権利、条件およびユーザを含む、SRL308内の権利データを、関連コンテンツを変更せずに更新することができる。具体的には、再公表は、関連コンテンツを新しい（CK）で再暗号化する必要はない。また、再公表は、元のSRL308が新しいSRL308にコピーされる多数のアイテムを有するために、最初から新しいSRLを生成する必要はない。

#### 【0092】

（署名付き権利ラベル308の自己公表）

本発明の一実施形態では、SRL308は、要求側ユーザ自身によって署名することができる。従って、ユーザは、DRMサーバ320に連絡し、関連するコンテンツの一部分のSRL308を取得する必要はない。その結果、自己公表（Self-Publishing）は、オフラインの公表とも呼ばれている。このような実施形態では、ユーザは、DRM320に連絡することが要求され、自己公表されたSRL308に基づいたライセンスを要求する。当然に理解されるように、公表エンティティは、独自のライセンスを発行することができる。

#### 【0093】

具体的には、図10に示すように、この実施形態では、ユーザは、DRMサーバ320からDRM証明書810を受け取ることにより、自己公表する用意ができる。DRM証明書810は、公開鍵（PU-CERT）、およびユーザの公開鍵（PU-ENTITY）に従って暗号化され、その結果として（PU-ENTITY（PR-CERT））となる対応する秘密鍵（PR-CERT）とを含む。証明書は、DRMサーバ320の秘密鍵（PR-DRM）で署名され、以下で詳しく説明するように、そのDRMサーバ320がそれを検証することができる。当然に理解されるように、DRM証明書810は、ユーザが自己公表するのを許可する。当然に理解されるように、鍵ペア（PU-CERT, PR-CERT）は、（PU-ENTITY, PR-ENTITY）とは別で、特に自己公表のために使用される。

なお、鍵ペア（PU-CERT, PR-CERT）は使用しないで済むこともあり、その場合には、DRM証明書810は、ユーザの公開鍵（PU-ENTITY）だけを含み、DRMサーバ320の秘密鍵（PR-DRM）で署名され、そのDRMサーバがそれを検証することができる。

#### 【0094】

自己公表は、ユーザがそれにより実行されるステップに関してDRMサーバ320に代わる点で、図4に示す公表と異なっている。特に、ユーザが、提出された権利ラベルに署名し、その結果として署名付き権利ラベル（SRL）308となることである。提出された権利ラベルは、DRM証明書810から取得された（PR-CERT）（つまり、S（PR-CERT））とともに、（PU-DRM（DES1））と（DES1（r19h7Sdα7α））とを含む。当然に理解されるように、ユーザは、DRM証明書810から（PU-ENTITY（PR-CERT））を取得し、それに（PR-ENTITY）を適用することによって、DRM証明書810から（PR-CERT）を取得する。ここで注意すべきことは、ユーザが（PU-DRM（DES1））に適用する（PR-DRM）を有していないために、ユーザは、DRMサーバ320が提出された権利ラベルの権利を実施することができるという検証をすることができない。従って、DRMサーバ320自身は、ライセンスが自己公表されたSRL308に基づいて要求された時点で、その検証を行う必要がある。

#### 【0095】

ユーザがSRL308を自己公表すると、ユーザは、その自己公表されたSRL308と、そのコンテンツと同じものを生成するために使用されたDRM証明書810とを連結し、SRL308とDRM証明書810付きのコンテンツは、別のユーザに配信される。そ

10

20

30

40

50

の後、別ユーザは、コンテンツのライセンスを、図7と図8に示す同じ方法で、DRMサーバ320に要求し、取得する。ここでは、ライセンスを要求するユーザは、自己公表されたSRL308とコンテンツに連結されたDRM証明書810の両方を、DRMサーバ320に提出する。DRMサーバ320は、DRM証明書810の中のS(PR-DRM)を、対応する(PU-DRM)に基づいて検証し、DRM証明書810から(PU-CERT)を取得する。次に、DRMサーバ320は、SRL308の中のS(PR-CERT)を、取得した(PU-CERT)に基づいて検証し、上述したように続ける。当然に理解されるように、ユーザは、DRMサーバ320がSRL308の中の権利を実施できることを検証できないので、上述したように、DRMサーバ320自身が、その時点で検証を行う必要がある。

【0096】

(権利テンプレート)

上述したように、ユーザまたはユーザクラスを定義し、定義されたユーザまたはユーザクラスの各々に権利を定義し、使用条件を定義することにより、ほとんどの、どのような種類の権利データでも権利ラベルの中に生成する自由度が、ユーザに与えられている。しかし、重要なことは、特に、同じユーザまたはユーザクラス、権利および条件が、コンテンツの異なる部分ごとに繰り返し定義されるとき、複数の権利ラベルの権利データを繰り返し定義することは、煩わしく、反復的になる。このようなことは、例えば、企業やオフィス環境で起こっており、ここでは、ユーザは、定義された特定のユーザチームと共有される、コンテンツの異なる部分を繰り返し公表する。このような状況で、本発明の一実施形態では、権利テンプレートが作成され、ユーザは、権利ラベルを作成することに関して繰り返し使用することができ、ここでは、権利テンプレートは、事前に定義されたユーザまたはユーザクラス、事前に定義された各ユーザまたはユーザクラスの権利、および事前に定義された使用条件を含む。

【0097】

本発明の一実施形態では、図11に示すように、権利テンプレート900は、権利ラベルの中の権利データと実質的に同じである。しかし、(DES1)は、コンテンツが公表されるまでは分からないので、権利データを、権利ラベルの場合と同じように、その(DES1)に従って暗号化することはできない。本発明の一実施形態では、暗号化されていない権利データを有する権利テンプレートを、図4のステップ416において(DES1)で権利データを暗号化する過程において提出し、(DES1(ri9h7sda7a))を生成する。もちろん、権利データは、暗号化される前に、提出された権利テンプレート900から取り出される。

【0098】

DRMサーバ320とその公開鍵(PU-DRM)は、権利テンプレートが構成される時に分かっている場合と、分かっている場合とがある。さらに、分かっている場合でも、各々が独自の(PU-DRM)を有するDRMサーバ320が2つ以上存在する場合と、存在しない場合とがある。それにもかかわらず、DRMサーバ320とその公開鍵(PU-DRM)が権利テンプレートの構築時に分かっている場合や、1つのDRMサーバ320だけが採用されているが、または権利テンプレート900に関連して1つのDRMサーバだけが採用されるような場合には、権利テンプレートは、権利テンプレート900から得られる権利ラベルに署名しようとするDRMサーバに関する情報であって、公開鍵(PU-DRM)を含む情報を含むことができる。この(PU-DRM)は、(DES1)を暗号化し、その結果として(PU-DRM(DES1))を得るものとして、SRL308に入っているが、当然に理解されるように、(DES1)は、コンテンツが公表されるまで分かっている場合と、権利テンプレート900の中の(PU-DRM)は、権利ラベルの場合と同じように、その(DES1)を暗号化することができない。本発明の一実施形態では、暗号化されていない(PU-DRM)を有する権利テンプレートを、図4のステップ414において(PU-DRM)で(DES1)を暗号化している過程で提出し、(PU-DRM(DES1))を生成する。もちろん、(PU-DRM)は、使用される

前に、提出された権利テンプレート 900 から取り出される。

【0099】

また、上述のケースでは、権利テンプレートに含むことができる DRMサーバに関する他の情報は、ネットワーク上の DRMサーバを探し出すための URL などの照会情報、および URL が失敗したときのフォールバック情報を含むことができる。どの場合にも、権利テンプレートは、権利テンプレート 900 自体を記述した情報を含むことができる。なお、権利テンプレート 900 は、コンテンツおよび/または暗号化鍵 (CK) と (DES1) とに関する権利ラベルに記述される情報などの、公表されるコンテンツに関する情報が入るスペースを提供することもできるが、権利テンプレートをインスタンス化したものが、実際には権利ラベルに変換されるのでなければ、そのスペースは不要である。

10

【0100】

これまでに説明してきた権利テンプレートは、主にユーザの便宜のためのものであるが、当然に理解されるように、事情によっては、ユーザが、権利ラベルに権利データを定義する自由度を制限すべきであり、権利テンプレート 900 を使用して、生成される権利ラベルの範囲または種類を制限することができる。例えば、特に企業またはオフィス環境の場合には、特定のユーザが、常にコンテンツを特定のユーザクラスにのみ公表すべきこと、またはユーザが、コンテンツを特定のユーザクラスに公表してならないポリシーとして、事前に定義しておくことができる。いずれの場合も、本発明の一実施形態では、このようなポリシーを、事前定義された権利データとして 1 または複数の権利テンプレート 900 に具現化し、ユーザが、コンテンツを公表するとき、その権利テンプレートを使用して権利ラベルを生成するのを制限することができる。特に、権利テンプレートまたは権利テンプレート群は、ユーザが、本発明の精神と範囲から逸脱しない限り、あらゆる種類の公表ポリシーを指定することができるように、ユーザが公表ポリシーを利用可能にする。

20

【0101】

制限されたユーザなどの権利テンプレート 900 を指定するために、図 12 を参照して説明すると、アドミニストレータなどは、実際には、事前定義された権利データを定義し (ステップ 1001)、特定の DRMサーバ 320 に関する情報などの、必要で、かつ適当な他の情報を定義する (ステップ 1003) ことにより、権利テンプレート 900 を構築する。重要なことは、限定されたユーザなどによって使用される権利テンプレートをもたらすためには、権利テンプレート 900 を公的にしなければならぬ。すなわち、権利テンプレート 900 は、限定ユーザなどが採用できる権利テンプレートとして認識しなければならない。従って、本発明の一実施形態では、アドミニストレータなどによって構築された権利テンプレートは、DRMサーバ 320 に提出され、これにより署名され、この署名は、権利テンプレートを公的なものにす (ステップ 1005)。

30

【0102】

署名する DRMサーバ 320 は、その情報が実際に権利テンプレート 900 に存在するとき、その情報が権利テンプレート 900 にある DRMサーバ 320 のことである。また、DRMサーバ 320 は、必要なチェックを行ったときだけ権利テンプレート 900 に署名することができる、まったくチェックなしで署名することもできる。さらに、DRMサーバからのテンプレート署名 S (PR-DRM-T) (ただし、-T は、署名が ORT 900 に対するものであることを意味している) は、少なくとも権利テンプレート 900 の事前定義された権利データに基づくべきであるが、本発明の精神と範囲から逸脱しない限り、他の情報に基づくこともできる。以下で説明するように、署名 S (PR-DRM-T) は、権利ラベルの中に組み込まれ、権利ラベルに関連して検証され、従って、署名が基づくものがあれば、変更されない形で権利ラベルの中に組み込まれるべきである。

40

【0103】

DRMサーバ 320 が権利テンプレート 900 に署名し、それをアドミニストレータなどに戻すと、アドミニストレータは、署名され、いまは公的になっている権利テンプレート 900 を S (PR-DRM-T) とともに受け取り (ステップ 1007)、公的権利テンプレート (ORT) 900 を 1 または複数のユーザに転送し、そのユーザによって使用す

50

れる（ステップ1009）。従って、ユーザがORT900に基づいてコンテンツを公表するために、ユーザは、ORT900を取り出し（ステップ1011）、あらゆる必要とされる情報を用意することによって、ORT900に基づいて権利ラベルを構築する（ステップ1013）。必要とされる情報は、コンテンツに関する情報、適当な鍵情報、（DES1）によってORT900から暗号化されると、結果として（DES1（*アイダムセダセ*））となる権利データ、およびORT900からの他の情報などである。重要なことは、ユーザは、ORT900からの署名S（PR-DRM-T）を権利ラベルに含む。

#### 【0104】

そのあと、上述したように、ユーザは、署名のために権利ラベルをDRMサーバ320に提出する（ステップ1015）。なお、ここでは、DRMサーバ320は、その中のS（PR-DRM-T）が検証されなければ、提出された権利ラベルに署名しない。すなわち、DRMサーバ320は、提出された権利ラベルが、ORT900からの署名S（PR-DRM-T）を含まなければ、提出された権利ラベルに署名することを拒否することにより、ユーザが、提出された権利ラベルをORT900に基づくべきことを強制する。具体的には、DRMサーバ320は、そのS（PR-DRM-T）と、その署名に基づいている情報があれば、提出された権利ラベルから取り出し、（PU-DRM）に基づいてその署名を検証する。提出された権利ラベルの権利データは、（DES1）に従って暗号化されている（すなわち、DES1（*アイダムセダセ*））。従って、DRMサーバ320は、図9を参照して上述したように、最初に（DES1）を取得し、それを使用して（DES1（*アイダムセダセ*））を解読し、提出された権利ラベルの権利データに基づいて署名を検証することができる。

#### 【0105】

検証されると、DRMサーバ320は、上述したように、S（PR-DRM-L）を使用して、提出された権利ラベルに署名し、SRL308を生成する（ただし、-Lは、署名がSRL308に対するものであることを意味している）。ここで、S（PR-DRM-L）は、S（PR-DRM-T）を置き換えることも、S（PR-DRM-T）に付加されることもある。付加されるときは、S（PR-DRM-L）は、S（PR-DRM-T）の一部に基づくことができる。（PR-DRM）は、S（PR-DRM-T）とS（PR-DRM-L）の両方を得るために使用することができるが、異なる（PR-DRM）を、S（PR-DRM-T）とS（PR-DRM-L）の各々に使用することもできる。DRMサーバ320が権利ラベルに署名し、SRL308をユーザに戻すと、ユーザは、S（PR-DRM-L）とともにSRL308を受け取り（ステップ1017）、上述したように、そのSRL308を公表しようとするコンテンツと連結する処理に進む。

#### 【0106】

ORT900の署名S（PR-DRM-T）が、少なくともORT900の事前定義された権利データの一部に基づいている場合には、SRL308に（DES1（*アイダムセダセ*））に入っている権利データは修正すること、変更することできない。そうでなければ、S（PR-DRM-T）は検証されない。それにもかかわらず、本発明の実施形態では、ORT900の中の権利データは、ORT900に含まれる規定されたルール内で変更することができる。例えば、ルールは、2つの権利データセットの1つを、SRL308に含めることを指定し、または別のセットの中から選択を可能にすることもできる。当然に理解されるように、ルールは、本発明の精神と範囲から逸脱しない限り、適当なシンタックスで記述された、どのようなルールにすることもできる。ここでは、ルールは、権利ラベルの作成時に、ユーザの適当なルールインタフリティによって解釈される。権利データは、変化することがあるが、ルールは同じように変化しないので、ORT900のテンプレートの署名S（PR-DRM-T）は、権利データ自体ではなく、少なくともルールの一部に基づいている。その結果、ORT900に含まれるルールは、SRL308に含まれていなければならない。

#### 【0107】

10

20

30

40

50

本発明の一実施形態では、O R T 9 0 0 の事前定義された権利データは、上述したように、一部が固定で、不変であり、一部が可変で、ルール駆動 (rule-driven) になっている。ここでは、O R T 9 0 0 のテンプレート署名 S (P R - D R M - T) は、少なくともルールの固定部分の一部に基づき、権利データの可変部分のルールに基づいている。

#### 【0108】

当然に理解されるように、ユーザが所有している O R T 9 0 0 は、時代遅れになるか、あるいは陳腐化することがある。すなわち、権利データを通して O R T 9 0 0 は、最新でなくなり、無関係となり、あるいは単純に適用できなくなったポリシーを反映していることがある。例えば、O R T 9 0 0 の権利データの中で指定されている 1 または複数のユーザまたはユーザクラスは、ポリシー環境内に最早存在していないこともあれば、O R T 9 0 0 の権利データの中で指定された特定のユーザまたはユーザクラスは、ポリシー環境内で最早同じ権利を有していないこともある。そのようなケースでは、アドミニストレータが、改訂された O R T 9 0 0 を発行したが、ユーザは、旧版で、時代遅れの O R T 9 0 0 をまだ使用していることがある。

#### 【0109】

このような状況で、本発明の一実施形態では、D R M サーバ 3 2 0 が、提出された権利テンプレート 9 0 0 に署名して O R T 9 0 0 を生成し、O R T 9 0 0 のコピーを保存しておくと、各 O R T 9 0 0 は、ユニークな識別インデックスが付けられ、O R T 9 0 0 に基づいて構築された各権利ラベルは、その O R T 9 0 0 の識別インデックスを含む。従って、図 1 2 に示すように、提出された権利ラベルを受け取ると、D R M サーバ 3 2 0 は、権利ラベルの中から O R T 9 0 0 の識別インデックスを見つけ、見つかった識別インデックスに基づいて O R T 9 0 0 の最新コピーを取り出し、提出された権利ラベルから権利データを削除し、取り出した O R T 9 0 0 から権利データを挿入し、最後に、少なくとも挿入された権利データの一部に基づいた権利ラベルに署名する。もちろん、D R M サーバは、(D E S 1 (1976)) を解読し、再暗号化することを含み、上述したプロセスの中で必要とされ、義務付けられ暗号化と平文化ステップを実行する。D R M サーバが、提出された権利ラベルの権利データを置換するように構成されているときには、その権利ラベルと、その権利ラベルが構築される基となった O R T 9 0 0 とは、必ずしも、権利データを含む必要はない。その代わりに、権利データは、D R M サーバ 3 2 0 に置いておく必要がある。しかし、権利データを権利ラベルおよびその権利ラベルが構築される基となった O R T 9 0 0 に含めることは、ユーザにとっては好都合であり、事情によっては有用なことがある。

#### 【0110】

##### (結論)

本発明に関連して実行されるプロセスを実現するために必要なプログラミングは相対的に単純明快であり、プログラミング関係者には自明のはずである。従って、このようなプログラミングは、本明細書には添付していない。そこで、本発明の精神と範囲を逸脱しない限り、どのようなプログラミングを採用しても、本発明を実現することが可能である。

#### 【0111】

以上、デジタルコンテンツとサービスに対する使用ライセンスを、署名付き権利ラベルを通して発行するためのシステムと方法を説明してきた。当業者ならば理解されるように、本発明の好適実施形態は、様々な態様に変更し、改良することが可能であり、かかる変更と改良は本発明の範囲から逸脱しない形で行うことができる。従って、請求項に記載されている本発明の範囲には、かかる等価的な変形のすべてが含まれる。

#### 【0112】

付録 1

#### 【0113】

##### 【表 3】



## 権利データの例

```

<?xml version="1.0" ?>
<XrML version="1.2">
  <BODY type="Rights Template">
    <DESCRIPTOR>
      <OBJECT>
        <ID type="GUID">c43...</ID>
        <NAME>$$411$411name$411desc</NAME>
      </OBJECT>
    </DESCRIPTOR>
    <WORK>
      <OBJECT>
        <ID />
      </OBJECT>
      <RIGHTSGROUP name="MAIN RIGHTS">
        <RIGHTSLIST>
          <VIEW>
            <CONDITIONLIST>
              <ACCESS>
                <PRINCIPAL>
                  <OBJECT>
                    <ID />
                    <NAME>test@company.com</NAME>
                  </OBJECT>
                </PRINCIPAL>
              </ACCESS>
            </CONDITIONLIST>
          </VIEW>
          <RIGHT name="generic">
            <CONDITIONLIST>
              <ACCESS>
                <PRINCIPAL>
                  <OBJECT>
                    <ID />
                    <NAME>test@company.com</NAME>
                  </OBJECT>
                </PRINCIPAL>
              </ACCESS>
            </CONDITIONLIST>
          </RIGHT>
        </RIGHTSLIST>
      </RIGHTSGROUP>
    </WORK>
  </BODY>

```

10

20

30

40

【 0 1 1 4 】

【 表 4 】

```
<SIGNATURE>
  <ALGORITHM>RSA PKCS#1-V1.5</ALGORITHM>
  <DIGEST>
    <ALGORITHM>SHA1</ALGORITHM>
    <PARAMETER name="codingtype">
      <VALUE encoding="string">surface-coding</VALUE>
    </PARAMETER>
    <VALUE encoding="base64" size="160">MwI...=</VALUE>
  </DIGEST>
  <VALUE encoding="base64" size="1024">Msi...=</VALUE>
</SIGNATURE>
</XrML>
```

10

【 0 1 1 5 】

付 録 2

【 0 1 1 6 】

【 表 5 】

## 署名付き権利ラベル 3 0 8 の例

```

<?xml version="1.0" ?>
<XrML version="1.2">
  <BODY type="Rights Label" version="3.0">
    <ISSUEDTIME>2002-01-01_12:00:00</ISSUEDTIME>
    <DESCRIPTOR>
      <OBJECT>
        <ID />
        <NAME>$$409$...</NAME>
      </OBJECT>
    </DESCRIPTOR>
    <ISSUER>
      <OBJECT type="DRM-Server">
        <ID type="GUID">{d81...}</ID>
        <NAME>Test DRM Server</NAME>
        <ADDRESS type="URL">http://licensing.dev.com</ADDRESS>
      </OBJECT>
      <PUBLICKEY>
        <ALGORITHM>RSA</ALGORITHM>
        <PARAMETER name="public-exponent">
          <VALUE encoding="integer32">65537</VALUE>
        </PARAMETER>
        <PARAMETER name="modulus">
          <VALUE encoding="base64" size="1024">NcO...=</VALUE>
        </PARAMETER>
      </PUBLICKEY>
      <ENABLINGBITS type="sealed-key">
        <VALUE encoding="base64" size="1024">tFg...=</VALUE>
      </ENABLINGBITS>
      <SECURITYLEVEL name="Server-Version" value="2.0" />
      <SECURITYLEVEL name="Server-SKU" value="22222-3333" />
    </ISSUER>
    <DISTRIBUTIONPOINT>
      <OBJECT type="LICENSE ACQUISITION URL">
        <ID type="GUID">{0F4...}</ID>
        <NAME>DRM Server Cluster</NAME>
        <ADDRESS type="URL">http://localhost/Licensing</ADDRESS>
      </OBJECT>
    </DISTRIBUTIONPOINT>
    <WORK>
      <OBJECT type="TEST-FORMAT">
        <ID type="MYID">FDB-1</ID>
      </OBJECT>
    <METADATA>
      <SKU type="PIDTYPE">PID</SKU>

```

10

20

30

40

【 0 1 1 7 】

【 表 6 】

```

</METADATA>
<PRECONDITIONLIST>
  <TIME />
</PRECONDITIONLIST>
</WORK>
<AUTHDATA name="Encrypted Rights data">PAB... </AUTHDATA>
</BODY>
<SIGNATURE>
  <ALGORITHM>RSA PKCS#1-V1.5</ALGORITHM>
  <DIGEST>
    <ALGORITHM>SHA1</ALGORITHM>
    <PARAMETER name="codingtype">
      <VALUE encoding="string">surface-coding</VALUE>
    </PARAMETER>
    <VALUE encoding="base64" size="160">Prc...=</VALUE>
  </DIGEST>
  <VALUE encoding="base64" size="1024">EHd...=</VALUE>
</SIGNATURE>
</XrML>

```

10

20

#### 【図面の簡単な説明】

【図 1】本発明を実現することができ、この環境に限定されない例示コンピューティング環境を示すブロック図である。

【図 2】本発明を実現することができ、種々のコンピューティングデバイスが置かれていた例示ネットワーク環境を示すブロック図である。

【図 3】デジタルコンテンツを公表するための本発明にかかるシステムと方法の好適実施形態を示す機能ブロック図である。

【図 4】権利管理されたデジタルコンテンツを公表するための本発明にかかる方法の好適実施形態を示すフローチャートである。

30

【図 5】図 4 の方法によって作成された署名付き権利ラベルの構造を示すブロック図である。

【図 6】権利管理されたデジタルコンテンツをライセンスするための本発明にかかるシステムと方法の好適実施形態を示す機能ブロック図である。

【図 7】権利管理されたデジタルコンテンツをライセンスするための本発明にかかる方法の好適実施形態を示すフローチャートである。

【図 8】権利管理されたデジタルコンテンツをライセンスするための本発明にかかる方法の好適実施形態を示すフローチャートである。

【図 9】本発明の一実施形態に従って権利ラベルを再公表するとき実行される主要ステップを示すフローチャートである。

40

【図 10】ユーザが本発明の一実施形態に従ってオフラインの公表の実行を可能にするために DRMサーバによりユーザに発行される証明書を示すブロック図である。

【図 11】本発明の一実施形態にしたがって権利ラベルに組み込まれる情報を指定している権利テンプレートを示すブロック図である。

【図 12】本発明の一実施形態に従って図 11 の権利テンプレートを生成し、権利テンプレートに基づいて図 5 の署名付き権利ラベルを生成するときに実行される主要ステップを示すフローチャートである。

【図 13】トラストベースシステムの例の実施アーキテクチャを示すブロック図である。

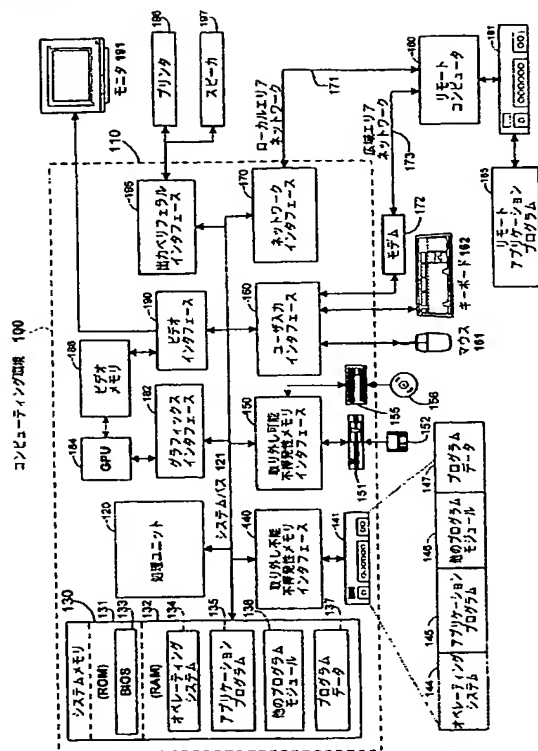
#### 【符号の説明】

300 クライアントデバイス

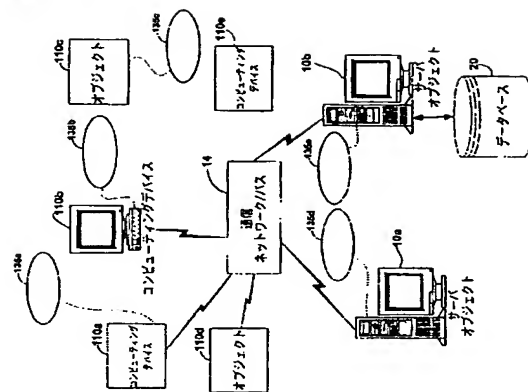
50

- 302 コンテンツ準備アプリケーション
- 304 暗号化デジタルコンテンツファイル
- 306 DRMクライアントAPI
- 308 署名付き権利ラベル(SRL)
- 310 権利管理デジタルコンテンツファイル
- 320 DRMサーバ
- 330 通信ネットワーク

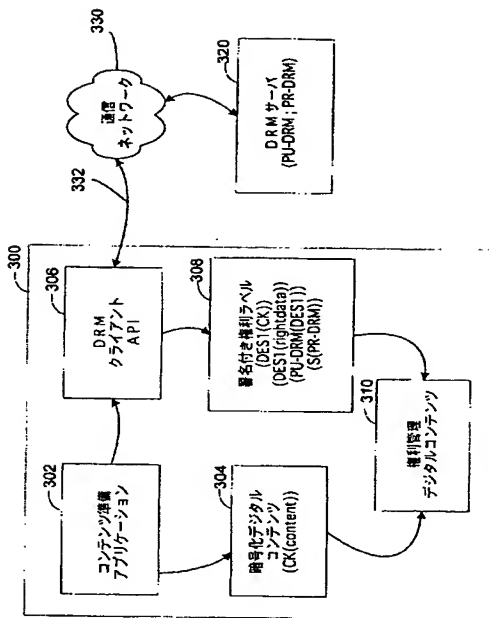
【図1】



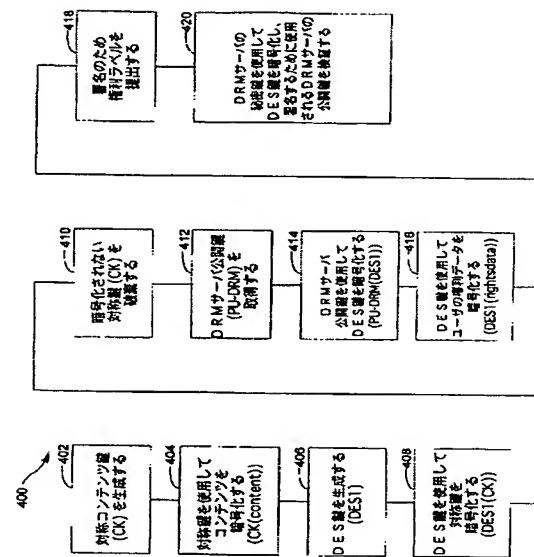
【図2】



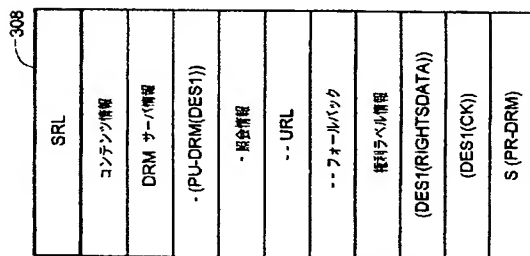
【図 8】



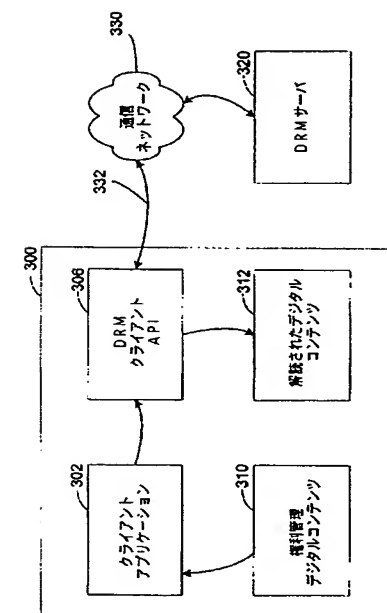
【図 4】



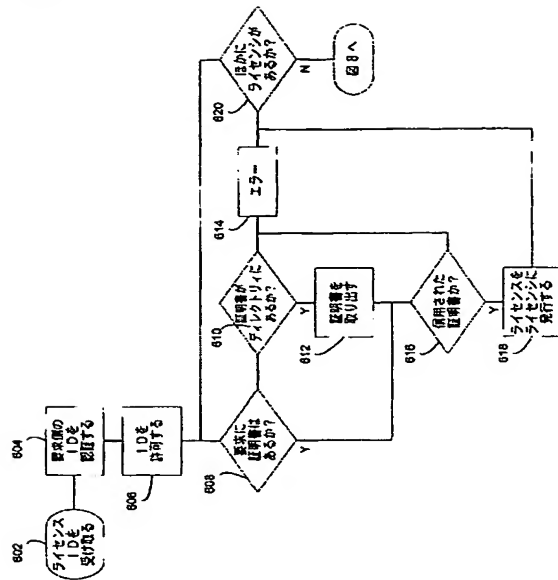
【図 5】



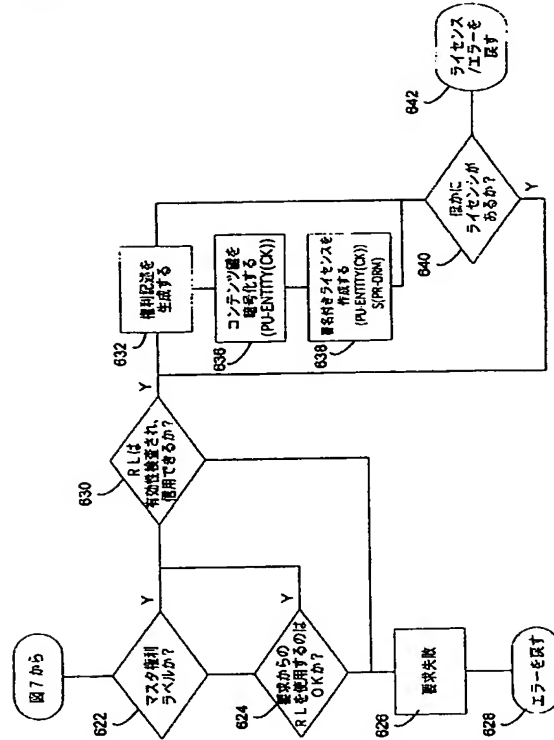
【図 6】



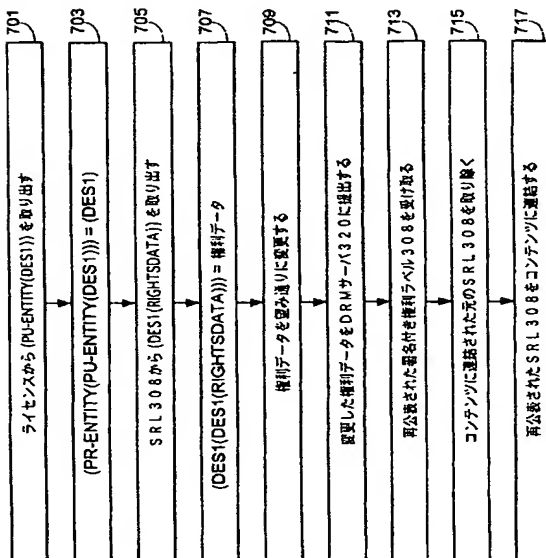
【図 7】



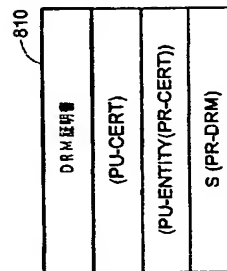
【図 8】



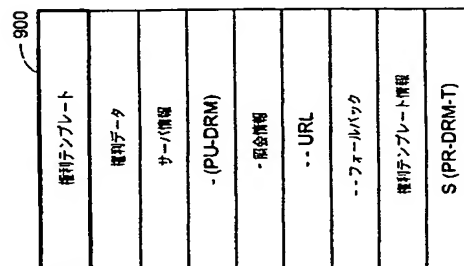
【図 9】



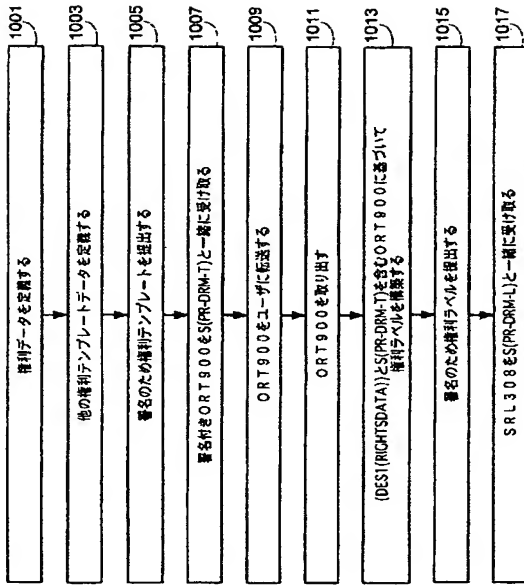
【図 10】



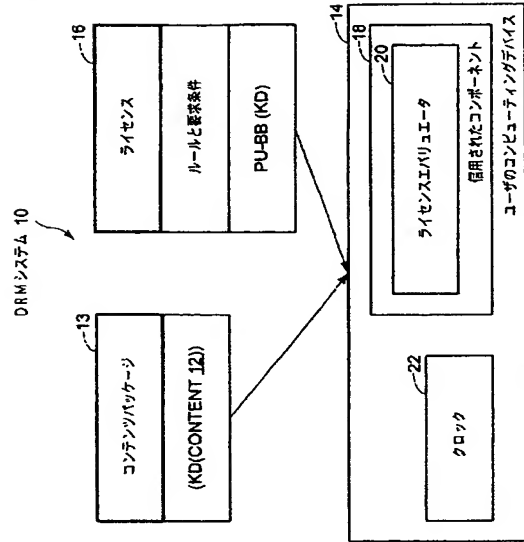
【図 11】



【図 1 2】



【図 1 3】





## フロントページの続き

(72)発明者 バラシャント マリク  
アメリカ合衆国 98052 ワシントン州 レッドモンド 156 アベニュー ノースイース  
ト 4850 ナンバー313

(72)発明者 ビネー クリシュナスワミー  
アメリカ合衆国 98072 ワシントン州 ウォディンビル ノースイースト 142 プレイ  
ス 23319

(72)発明者 ジェームズ ビー. ショープ ジュニア  
アメリカ合衆国 98103 ワシントン州 シアトル イースタン アベニュー ノース 44  
13

(72)発明者 チャンドラモウリ ベンカテシュ  
アメリカ合衆国 98074 ワシントン州 サマミッシュ 213 プレイス サウスイースト  
414

(72)発明者 アチャラ ナリン  
アメリカ合衆国 98011 ワシントン州 ホズエル ノースイースト 144 コート 87  
41

Fターム(参考) 5B017 AA07 BA06 CA16

5J104 AA01 AA07 AA09 AA12 AA16 EA01 EA04 EA15 EA18 JA03

JA21 KA01 KA05 KA15 LA03 LA06 MA01 NA02 NA37 PA14

**THIS PAGE BLANK (USPTO)**